KESKITETYN KÄYTTÄJÄHALLINNAN SUUNNITTELU JA TOTEUTTAMINEN KANSANELÄKELAITOKSEN AKTIIVILAITTEISIIN

Juho Myllys

Opinnäytetyö
Syyskuu 2013

Tietotekniikan koulutusohjelma
Tekniikan ja liikenteen ala

JYVÄSKYLÄN AMMATTIKORKEAKOULU
JAMK UNIVERSITY OF APPLIED SCIENCES

JYVÄSKYLÄN AMMATTIKORKEAKOULU
JAMK UNIVERSITY OF APPLIED SCIENCES

KUVAILULEHTI

Tekijä(t) MYLLYS, Juho	Julkaisun laji Opinnäytetyö	Päivämäärä 12.9.2013
	Sivumäärä 113 + 63	Julkaisun kieli Suomi
		Verkkojulkaisulupa myönnetty (X)

Työn nimi
KESKITETYN KÄYTTÄJÄHALLINNAN SUUNNITTELU JA TOTEUTTAMINEN KANSANELÄKELAITOKSEN AKTIIVILAITTEISIIN

Koulutusohjelma
Tietotekniikan koulutusohjelma

Työn ohjaaja(t)
SAHARINEN, Karo

Toimeksiantaja(t)
Kansaneläkelaitos

Tiivistelmä
Opinnäytetyön toimeksiantajana toimi Kansaneläkelaitos. Työ toteutettiin Kansaneläkelaitoksen IT-osastolle. Opinnäytetyön tavoitteena oli suunnitella ja toteuttaa toimeksiantajan laboratorioympäristöön toimiva keskitettykäyttäjähallinta aktiivilaitteisiin. Suunnittelu piti sisällään protokollan kartoittamisesta aina toteuttamiseen saakka erilaiset osa-alueet, kuten konfiguraatoiden ja konfiguroinnin suunnittelun. Opinnäytetyön yhtenä osa-alueena oli myös ottaa huomioon VAHTI-ohjeen eri osa-alueet liittyen tietoverkkoon.

Työssä saavutettiin kattava suunnitelma keskitetylle käyttäjähallinnalle, jonka avulla pystyttiin toteuttamaan kyseinen toiminto vaivattomasti. VAHTI-ohjeen osalta työssä ohjelmoitiin erilaisia skriptejä, joiden avulla pystyttiin lisäämään käytettävyyttä verkolle, kuten laitteiden varmuuskopioinnin automatisointi. Konfigurointiin suunniteltiin skripti jonka avulla olemassa olevat laitteet pystyttiin konfiguroimaan todella nopeasti ja vaivattomasti. Työssä myös mahdollistettiin erilaiset vaihtoehdot keskitetyn käyttäjähallinnan toimintojen tarkastelulle, kuten autentikaatioiden seuraamiselle web-sivuston kautta.

Lopputuloksena laboratorioympäristöön saatiin toteutettua verkko, josta keskitettykäyttäjähallinta, erilaisten osa-alueiden konfiguraatiot ja VAHTI-ohjeen osa-alueet ovat helposti implementoitavissa tuotantoympäristöön.

Avainsanat (asiasanat)
RADIUS, TACACS+, Varmuuskopio, SSH, Raportointi, Kansaneläkelaitos, VAHTI

Muut tiedot

JYVÄSKYLÄN AMMATTIKORKEAKOULU
JAMK UNIVERSITY OF APPLIED SCIENCES

DESCRIPTION

Author MYLLYS, Juho	Type of publication Bachelor´s Thesis	Date 12.9.2013
	Pages 113 + 63	Language Finnish
		Permission for web publication (X)

Title
Planning and implementation of centralized user management for network devices
CASE: the Social Insurance Institution of Finland

Degree Programme
Information Technology

Tutor(s)
SAHARINEN, Karo

Assigned by
KELA, Social Insurance Institution of Finland

Abstract
This bachelor's thesis was assigned by the Social Insurance Institution of Finland. The unit, for which the thesis was conducted was the IT department. The goal of this thesis was to design and implement centralized user management for the network devices in the client's laboratory environment. The designing part included features from comparing of protocols to the different field of implementation such as planning configurations of the devices and configuring them. A major research field of this thesis was to take care of different network parts of VAHTI-instruction.

The result of this thesis was a comprehensive plan for centralized user management, which enabled to carry out the function effortlessly. The parts of VAHTI-instruction made by programming different scripts made it possible to increase the usability of the network, such as backing up configurations of network devices. For the configuration of the network devices a script was designed to enable a really quick and easy configuration. This thesis also allowed to monitor different incidents of centralized user management such as authentications through a web site.

As a result, the laboratory environment was put online with centralized user management containing various aspects of the configuration and the VAHTI-instructions are now easily implemented in the production environment.

Keywords
RADIUS, TACACS+, Back up, SSH, Reporting, the Social Insurance Institution, VAHTI

Miscellaneous

SISÄLTÖ

KUVIOT

TAULUKOT

LYHENTEET

.exp	Expect –file
.sh	Shell –file
AAA	Authentication, Authorization & Accounting
ACL	Access Control List
ACS	Access Control Server
AD	Active Directory
AES	Advanced Encryption Standard
CLI	Command-Line Interface
CON	Console
DH	Diffie Hellman
DNS	Domain Name System
HMAC-SHA	Hash-based Message Authentication Code – Secure Hash Algorithm
IMC	Intelligent Management Center
IP	Internet Protocol
ISE	Identity Service Engine
KDC	Key Distribution Center
KPASSWD	Kerberos Password
L2/L3	OSI -viitemallin osoittama toiminnallisuustaso (Layer)
LDAP	Lightweight Directory Access Protocol
MD5	Message Digest 5
NAS	Network Access Server
NTP	Network Time Protocol
RADIUS	Remote Authentication Dial In User Service

RFC	Request For Comments
RSA	Ron Rivest, Adi Shamir & Leonard Adleman - salausalgoritmi
SCP	Secure Copy
SNMP	Simple Network Management Protocol
SSH	Secure Shell
TACACS	Terminal Access Controller Access-Control System
TCP	Transmission Control Protocol
TFTP	Trivial File Transport Protocol
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
VTY	Virtual TeletYpes
WWW	World Wide Web

1 LÄHTÖKOHDAT

1.1 Toimeksiantaja

Opinnäytetyön toimeksiantajana toimi Kansaneläkelaitos (jäljemmin Kela). Kelan tehtävänä on hoitaa Suomessa asuvien henkilöiden perusturvaa erilaisissa elämäntilanteissa. Kaikki Suomessa asuvat sekä ulkomailla asuvat Suomen sosiaaliturvan piiriin kuuluvat henkilöt ovat Kelan asiakkaita (Toiminta 2013).

Sosiaaliturvaan, jota Kela hoitaa, kuuluvat lapsiperheiden tuet, sairausvakuutus, kuntoutus, työttömän perusturva, asumistuki, opintotuki sekä vähimmäiseläkkeet. Edellä mainittujen lisäksi Kela huolehtii vammaisetuuksista, sotilasavustuksista ja maahanmuuttajan tuesta (Toiminta 2013).

Toimeksiantajana toimi tarkemmin ottaen Kelan IT-osasto. IT-osaston tehtävänä on erilaisten tietojärjestelmien suunnittelu, ylläpito, kehittäminen sekä tieto- ja viestintäteknologiajärjestelmien palveluiden tuottaminen, toimittaminen ja järjestäminen (Työjärjestys 2013). Toimeksiantajalla on kattava monitoimittajaympäristö verkossaan, jonka tiedonsiirtolaitteet koostuvat pääasiassa Dellin, HP:n ja Cisco Systemsin laitteista.

1.2 Tavoitteet

Opinnäytetyön tavoitteena oli selvittää toimeksiantajan toivomat osa-alueet liittyen aktiivilaitteiden käyttäjähallintaan, varmuuskopiointiin sekä luoda niistä toimiva laboratorioympäristö. Luodun ympäristön oli oltava helposti implementoitavissa tuotantoympäristöön. Keskeisin opinnäytetyön tavoite oli tutustua mahdollisiin protokolliin, joiden avulla voidaan toteuttaa keskitetty käyttäjähallinta verkon aktiivilaitteisiin, suojattu hallintayhteys sekä toimiva konfiguraatioiden varmuuskopiointi.

Aktiivilaitteiden hallintayhteyksissä ja varmuuskopioinneissa oli otettava huomioon valtionvarainministeriön asettamat ohjeet sisäverkolle. VAHTI sisäverkko-ohjeesta oli

tavoitteena ottaa niin paljon vaikutteita kuin mahdollista sekä pohtia niiden vaikutusta tietoturvaan.

Toimivassa laboratorioverkossa, jossa on toimiva keskitetty käyttäjähallinta, oli tarkoitus tutkia liikennöintiä eri laitteiden välillä (kytkin/reititin, RADIUS/TACACS – palvelin ja käyttäjähakemisto) mahdollisimman tarkasti. Laboratorioympäristössä olevan käyttäjähallinnan tulee hyödyntää ulkoista käyttäjätietokantaa. Toimeksiantajan tietoverkossa on suuri määrä aktiivilaitteita, jotka piti ottaa huomioon ja tästä syystä työssä pyrittiin suunnittelemaan ratkaisu, joka helpottaa laitteiden konfiguraatioita.

2 AAA

2.1 Yleistä

AAA-arkkitehtuuri koostuu nimensä mukaisesti kolmesta A:sta, jotka ovat Authentication (Tunnistaminen), Authorization (Valtuuttaminen) sekä Accounting (Kirjanpito). Santuka (2013 chapter 1) kertoo, että AAA-protokolla voidaan ajatella sillä tavalla, että kuka olet (Authentication), mitä saat tehdä (Authorization) ja mitä teit sillä välin, kun olit täällä (accounting). Santuka neuvoo katsomaan RFC-dokumenttia 2903, joka käsittelee yleisesti AAA-arkkitehtuuria.

2.2 Authentication

Ensimmäisenä AAA-arkkitehtuurin osiona on *Authentication* eli tunnistautuminen. Santuka (2013, chapter 1, Authentication overview) kertoo arkipäivän esimerkkinä kirjassaan autentikoinnista, että olet menossa elokuvateatteriin katsomaan elokuvaa, johon olet ostanut lipun. Ovella henkilökunta pyytää sinua näyttämään lipukkeen ja näytät sen, jotta pääset sisälle elokuviin. Teatterin ovimies on siis vaatinut sinulta jonkin tiedon, jolla pääset sisään teatteriin, eli hän suoritti autentikointiprosessin sinulle. Autentikaatio pohjautui johonkin, mitä sinulla on, eli elokuvalippuun. Autentikointitapahtumia voi olla muitakin, kuten mitä tiedät (salasana) tai mitä olet (sormenjälki). ’Mitä sinulla on’ -autentikointi voi olla esim. jaettu avain, jolla voit tunnistautua.

Verkon aktiivilaitteiden autentikoinnissa puhutaan pääasiassa autentikointitavasta ’mitä tiedät’. Yleinen autentikointitapa on joko käyttäjätunnus ja salasana -pari (mitä tiedät) tai käyttäjätunnus-avainpari (mitä sinulla on) tunnistus.

2.3 Authorization

Toisena AAA-arkkitehtuurin osiona on *Authorization* eli valtuuttaminen. Santuka (2013) kertoo kirjassaan valtuutuksesta esimerkkinä sen, että mikäli olet ostanut lennon ulkomaille 2. luokkaan, olet valtuutettu matkustamaan tällöin 2. luokassa, vaikka ykkösluokan mukavat matkustusolosuhteet houkuttelisivatkin. Valtuuttaminen on tapa tarjota eritasoisia oikeuksia käyttäjille. Keskitettyä käyttäjähallintaa miettiessä voi toinen käyttäjä mahdollisesti syöttää laitteille ainoastaan *show*-komentoja, kun taas toinen pystyy mahdollisesti suorittamaan konfiguraatioita laitteelle. Helpoin tapa suorittaa valtuuttamisen eri tasot on luoda ryhmiä, joilla on tietyt oikeudet ja näihin ryhmiin voidaan lisätä käyttäjiä, jotka saavat ryhmälle määritellyt oikeudet tiettyihin verkon palveluihin. (Santuka 2013)

2.4 Accounting

Viimeisenä AAA-arkkitehtuurin osiona on Accounting eli kirjanpito. Santuka (2013) kertoo kirjanpidosta esimerkkinä, että mennessäsi lentokoneeseen tietosi kirjataan lähtöselvityksessä ylös, jotta tiedetään, että olet saapunut lennolle. Kun Accounting-osio on käytössä, voivat aktiivilaitteet lähettää kirjanpitoon määritettyjä tapahtumia esimerkiksi ulkoiselle SYSLOG- tai RADIUS-palvelimelle riippuen konfiguraatioista (Santuka 2013).

AAA-arkkitehtuuri tukee monia erilaisia kirjanpitomahdollisuuksia, kuten verkkokirjanpito (Network accounting), joka tarjoaa tietoa erilaisista istuntotapahtumista. Yhteyskirjanpito (Connection accounting), joka tarjoaa tietoa ulkoa tulevista yhteyksistä kuten telnet-istunnoista. EXEC-kirjanpito (EXEC accounting) tarjoaa tietoa terminaali-istunnoista NAS-laitteille kuten käyttäjänimi, päivä, aloitus- ja lopetusajankohta sekä NAS-laitteen IP-osoitteen. Järjestelmäkirjanpito (System Accounting) tarjoaa tietoa eritasoisista järjestelmätapahtumista, kuten järjestelmän sammuttamisesta tai sen uudelleenkäynnistämisestä. Komentojen kirjanpito (Command Accounting) tarjoaa tietoa käyttäjien syöttämistä komennoista NAS-laitteeseen. Komentoja on mahdollis-

ta kirjata eritasoisilta käyttäjiltä. Esimerkiksi jos halutaan kirjata konfiguraatiomuutoksia, voidaan kirjata *privilege*-tason 15 komennot. Komentojen kirjanpidolla voidaan saada myös selville kuka komennon suoritti ja milloin, eli niin kutsuttu *Audit Trail* (Santuka 2013).

Esimerkkinä kirjanpidosta voisi olla tapahtuma, jossa valtuutettu käyttäjä lisää kytkimelle uuden *VLAN*in komennolla: *"vlan 30"*. Näin ollen komento kirjataan palvelimelle, joka on määritetty toimimaan kirjanpitopalvelimena.

3 TACACS VS. RADIUS

3.1 Yleistä

Tietoverkkojen toimintaa optimoidaan ja kehitetään jatkuvasti. Työasemat jaotellaan VLANien perusteella omiin verkkosegmentteihin, IP-osoitteet jaetaan keskitetyltä palvelimelta sekä monet muut asiat tietoverkoissa keskitetään palvelimille. Kyseinen asia tulee ottaa huomioon myös käyttäjähallintaa mietittäessä niin aktiivilaitteille kuin verkkoliikennöintiin. Aktiivilaitteiden käyttäjähallinnan suunnittelussa on otettava huomioon erilaisia asioita, joiden pohjalta voidaan tehdä päätös siitä, mitä verkkoon kannattaa lähteä rakentamaan. Halutaanko palvelimet kahdentaa, mitä protokollaa halutaan käyttää ja niin edelleen.

Aktiivilaitteiden käyttäjähallinnan perusasiat tulee ottaa huomioon. Näitä voivat olla mm. onko verkkolaitteisiin pääsyä eri osastoilta, kuten ylläpidosta ja valvonnasta, tai onko organisaatiossa hallinnollisesti kaksi tai useampaa eri puolta, joissa on omat osastonsa. Tämä on tärkeä asia, sillä eri osastoille halutaan usein antaa eritasoisia oikeuksia, kuten luku- ja/tai kirjoitusoikeudet.

3.2 Remote Authentication Dial In User Service

Remote Authentication Dial In User Service (RADIUS) protokolla on esitelty RFC-dokumentissa 2865, jossa kerrotaan RADIUS-protokollan perustoiminnasta, sekä RFC-dokumentissa 2866, joka on suunnattu RADIUS-protokollan accounting eli kirjanpito-osioon.

RADIUS toimii asiakas–palvelin-mallin mukaisesti, jossa asiakkaana toimii verkkolaite, ei siis itse loppukäyttäjä. Palvelimena toimii autentikointipalvelin, kuten Linux-palvelin, johon on asennettu RADIUS-lisäosa. Asiakaslaitetta kutsutaan usein nimellä NAS (*Network Access Server*), jonka vastuulla on välittää loppukäyttäjän tiedot määritetylle RADIUS-palvelimelle ja toimia palvelimen päätöksen perusteella. RADIUS-

palvelimen vastuulla on vastaanottaa loppukäyttäjän kannalta oleelliset viestit, todentaa käyttäjä sekä toimittaa oleelliset viestit NAS-laitteelle, joka puolestaan välittää tiedot loppukäyttäjälle (Rigney, Rubens Merit, Simpson Daydreamer & Willens Livingston 2013, 3).

RADIUS-palvelimen ja NAS-laitteen välinen kommunikointi perustuu jaettuun salaisuuteen, jota ei lähetetä koskaan verkon yli selkokielisenä. Loppukäyttäjän tunnistetiedoista vain salasana lähetetään salattuna verkossa, jotta mahdollinen murtautuja ei pääsisi näkemään käyttäjän salasanaa (Rigney ym. 2013, 3).

3.2.1 RADIUS-perustoiminta

Kun NAS-laitteelle on määritelty käytettäväksi RADIUS-protokolla, niin kaikki loppukäyttäjän autentikointitiedot lähetetään aluksi NAS-laitteelle, joka välittää viestit eteenpäin autentikaatiopalvelimelle. NAS-laite lähettää *Access-Request*-viestin, joka sisältää attribuutteja kuten loppukäyttäjän käyttäjätunnuksen ja salasanan, joita käyttäjä käyttää autentikoitumiseen. Salasanan liikkuessa verkon yli se suojataan käyttäen *MD5*-algoritmiä (Rigney ym. 2013, 3).

MD5-algoritmi on yksisuuntainen tiivistesummafunktio, eli tiivisteestä, jonka *MD5* tuottaa, on käytännössä mahdotonta saada selville alkuperäistä merkkijonoa. Molempien osapuolten tulee verrata tiivistettä keskenään, minkä perusteella tunnistetaan toinen osapuoli. Tiivistesumma on sama ainoastaan silloin, kun algoritmit ovat identtiset.

NAS-laitteen lähettämä *Access-Request*-viesti kuljetetaan aina RADIUS-palvelimelle tietoverkon kautta. Mikäli RADIUS-palvelin ei vastaa pyyntöön tietyssä ajassa, lähetetään *Access-Request*-viesti uudelleen niin montaa kertaa kuin se on NAS-laitteelle määritelty. Mikäli RADIUS-palvelimia on verkossa useampia kuin yksi, voidaan tällaisissa tapauksissa lähettää *Access-Request*-viesti vaihtoehtoiselle palvelimelle. Vaihtoehtoista palvelinta on mahdollisuus hyödyntää pelkästään varapalvelimena, tai voidaan useammalla palvelimella suorittaa kuormantasausta kiertovuorottelumenetelmällä eli niin sanotulla *Round-Robin* tavalla (Rigney ym. 2013, 5).

RADIUS-palvelimen saadessa *Access-request* pyynnön se vahvistaa NAS-laitteen luotettavuuden. Mikäli RADIUS-palvelin ei tunnista NAS-laitteen jaettua salaisuutta tai sitä ei ole, palvelin hylkää hiljaisesti NAS-laitteen pyynnön, toisin sanoen tästä ei jää minkäänlaisia lokimerkintöjä. Mikäli jaettu salaisuus löytyy ja se on pätevä, RADIUS-palvelin aloittaa loppukäyttäjän tietojen etsimisen määritellystä käyttäjätietokannasta (Rigney ym. 2013, 5).

Mikäli jokin autentikointiehdoista ei täyty, RADIUS-palvelin lähettää *Access-Reject*-viestin, joka ilmaisee että loppukäyttäjän *Access-Request* viesti oli virheellinen joltakin osin. Mikäli ensimmäinen *Access-Request*-viesti on hyväksytty ja RADIUS on käynnistänyt uuden istunnon, RADIUS lähettää *Access-Challenge*-viestin, johon NAS-laite vastaa toisella *Access-Request*-viestillä. Kaikkien ehtojen täytyttyä lähettää RADIUS-palvelin lopuksi *Access-Accept*-viestin eli hyväksymiseen tarkoitetun kuittausviestin. Vikatilanteessa RADIUS lähettää *Access-Reject*-viestin, jolloin loppukäyttäjän autentikaatio on epäonnistunut (Rigney ym. 2013, 5).

3.2.2 Haaste-vaste autentikointi

Haaste-vaste autentikoinnissa loppukäyttäjälle arvotaan sattumanvaraisesti jokin numero, jonka haastettu loppukäyttäjä salaa ja lähettää sen tuotoksen takaisin. RADIUS-palvelin vertaa tätä salausta omaansa ja mikäli kyseiset salatut arvot täsmäävät, autentikointi on onnistunut. Mikäli salatut arvot eivät vastaa toisiaan, yhteys katkaistaan.

3.2.3 RADIUS ja UDP

RADIUS käyttää kuljetukseensa UDP:tä (Used Datagram Protocol) eli yhteydetöntä protokollaa. Toisin kuin TCP, UDP ei huolehdi pakettien perille menosta. UDP:n heikkous onkin se, että viestiin ei koskaan saada kuittausta sen perille päästyä. RADIUS-protokollalle on kuitenkin valittu UDP kuljetusprotokollaksi tietyistä syistä.

Mikäli RADIUS-palvelin on vähintään kahdennettu, voi ilmaantua tilanteita, joissa pyynnöt ensisijaiselle RADIUS-palvelimelle eivät mene perille. Näin ollen pyynnöt täytyy ohjata toissijaiselle RADIUS-palvelimelle. Tällaisessa tapauksessa on pyynnön

kopio pidettävä kuljetustason yläpuolella, mikä sallii vaihtoehtoisen lähetyksen. Tämä kuitenkin tarkoittaa sitä, että tarvitaan ajastimet uudelleenlähetykselle (Rigney ym. 2013, 10).

RADIUS ei huolehdi kadonneesta tiedosta. Mikäli loppukäyttäjä suostuu odottamaan muutaman sekunnin autentikaatiota, TCP:n tarjoamalle uudelleenlähetykselle ei ole tarvetta eikä sen mukana tuleville vahvistussanomille. Toinen tilanne on, että mikäli käyttäjä ei suostu odottamaan useita minuutteja autentikaatiota, niin TCP:n tarjoamalle tiedolle viestien perille pääsystä parin minuutin kuluttua ei ole tarvita (Rigney ym. 2013, 10).

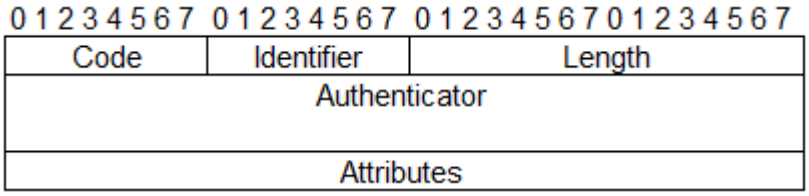
UDP:n takia RADIUS on niin sanotusti tilaton protokolla. NAS-laitteita sekä loppukäyttäjiä tulee ja menee, koneita sammutellaan sekä käynnistellään. TCP-protokollallekkaan tämä ei ole varsinaisesti ongelma, sillä koodia voidaan kirjoittaa siten, että se pystyy kestämään nämä tapahtumat, mutta UDP:n vahvuus on se, että se jättää huomioimatta nämä kyseiset seikat (Rigney ym. 2013, 10).

RADIUS -protokollan alkutaipaleella se pystyi prosessoimaan ainoastaan yhden pyynnön kerrallaan eli palvelin oli yksisäikeinen. Tästä muodostui ongelma ympäristöissä, joissa oli useita käyttäjiä, sillä palvelimen pyyntöjono täyttyi. Ratkaisu tähän oli kehittää palvelimesta monisäikeinen. UDP:n avulla tämä oli yksinkertaista. Jokaiselle loppukäyttäjälle, joka voi vastata UDP-paketilla suoraan NAS-laitteelle, perustettiin oma prosessi (Rigney ym. 2013, 11).

UDP vaatii ainoastaan yhden TCP:n ominaisuuden, eli uudelleenlähetyksen ajastimet samalle palvelimelle. Nämä ajastimet tulee luoda manuaalisesti, mikä teettää hieman ylimääräistä työtä. UDP tuo niin paljon muita etuja, että tämä on pieni haitta verrattuna UDP:n etuihin (Rigney ym. 2013, 101).

3.2.4 RADIUS paketin rakenne

RADIUS-paketin rakenne on esitelty kuviossa 1. Rakenne on melko yksinkertainen. Se koostuu kentistä *Code*, *Indentifier*, *Length*, *Authenticato*r sekä *Attributes*.



KUVIO 1. RADIUS-paketti

Code-kenttä on yhden oktetin mittainen ja identifioi RADIUS-paketin tyypin. Kun paketti saapuu ja siinä ei ole tunnistettavaa *Code*-kenttää, paketti hylätään hiljaisesti. RADIUS-protokollan *Code*-kentän arvot on esitelty taulukossa 1. *Code*-kentässä arvot 12 ja 13 ovat vielä toistaiseksi kehityksen alla.

TAULUKKO 1. *Code*-kentän arvoa vastaava tieto

1	Access-Request
2	Access-Accept
3	Access-Reject
4	Accounting-Request
5	Accounting-Response
11	Access-Challenge
12	Status-Server
13	Status-Client
255	Reserved

Identifier-kentän pituus on myös yksi oktetti. Tämän kentän tarkoituksena on auttaa oikeiden pyyntöjen ja vastauksien yhdistämisessä. RADIUS-palvelin voi tunnistaa päällekkäisyyksiä pyynnöistä, jos niissä on sama lähde-IP-osoite, lähde-UDP-portti ja tunnistestieto lyhyen ajan sisään (Rigney ym. 2013, 13).

Length-kenttä on kahden oktetin mittainen. Sen tehtävänä on osoittaa, kuinka pitkä paketin sisältö on kokonaisuudessaan. Mikäli *Length*-kentällä on pituutta yli kaksi oktettia, tulee loppuosa tulkita täytteenä ja hylätä. Mikäli paketti on lyhyempi kuin mitä *Length*-kenttä kertoo, se hylätään hiljaisesti (Rigney ym. 2013, 14).

Authenticator-kenttä on 16 oktettia pitkä. Nimensä mukaisesti kenttää käytetään palvelimen vastausten tunnistamiseen ja salasanojen salaamiseen. Kenttä jaetaan

karkeasti kahteen osaan, pyyntö- ja vastausarvot. Pyyntöarvossa kenttä on 16 oktettia pitkä ja sen arvo generoidaan sattumanvaraisesti. Lisäksi sen tulisi olla arvaamaton ja ainutlaatuinen koko olemassaolonsa ajan. RADIUS ei suojaa mitenkään kommunikointia, mikä helpottaa liikenteen salakuuntelua. Tähän ratkaisuna on edellämainittu täysin generoitu satunnaisluku. Satunnaisluvun ohessa tulee käyttää vahvaa salasanaa, jotka yhdessä tekevät murtautumisesta hankalaa (Rigney ym. 2013, 14).

Toinen arvo on vastausarvo jota käytetään *Access-Accept*, *Access-Reject* ja *Access-Challenge*-paketeissa. Tapahtumassa luodaan yksisuuntainen *MD5*-tiiviste, joka koostuu RADIUS-paketin otsakkeesta ja alkaa *Code*-kentällä. Edellä mainittu tiiviste pitää sisällään kentät *Identifier*, *Length*, *Request-authenticator*, *Attributes* ja *Secret.* Tätä kutsutaan termillä ”*ResponseAuht*” eli = *MD5(Code+ID+Length+RequestAuth+Attributes+Secret*), missä + tarkoittaa ketjuttamista (Rigney ym. 2013, 15).

3.2.5 RADIUS pakettien tyypit

RADIUS-paketin *Code*-kentän arvon ollessaan 1 on kyseessä viesti, jossa loppukäyttäjä haluaa liikennöidä verkossa eli *Access-Request*-viesti. *Access-Request*-viesti lähetetään RADIUS-palvelimelle, jonka tehtävänä on välittää käyttäjän tiedot NAS-laitteelle. Tiedot pitävät sisällään pääseekö käyttäjä verkkoon ja käyttäjän muista erikoisoikeuksista. *Identifier*- ja *Attributes*-kenttien tiedot muuttuvat aina kun *Access-Request*-viestiin vastataan. Uudelleen lähetyksessä Identifier-kentän sisällön on pysyttävä ennallaan. *Request-authenticator*-kentän arvon on aina muututtava kun uusi *Identifier*-arvo on käytössä. *Attributes*-kentän pituus on joustava ja se koostuu listasta erilaisia attribuutteja, jotka ovat tarpeellisia halutulle palvelulle (Rigney ym. 2013, 16 - 17).

Code-kentän arvon ollessaan 2 on kyseessä myöntävä vastaus oikeuksien pyytämiselle eli *Access-Accept*-viesti. Paketti lähetetään RADIUS-palvelimelta, mikäli *Access-Request*-viesteissä on ollut kaikki oleelliset asiat kunnossa. *Identifier*-kenttä on puhdas kopio *Access-Request*-viestin mukana tulleesta Identifier-kentästä, koska kyseessä on oikeuksien myöntäminen edellä olevalle pyynnölle. *Response Authenticator*-

kentän arvo on laskettu *Access-Request*-viestin arvosta, kuten aikaisemmin on esitetty kappaleessa 3.2.4. *Access-Accept*-viestin *Attributes*-kenttä on myös joustavan mittainen ja sen ei tarvitse sisältää yhtään attribuuttia (Rigney ym. 2013, 17 – 18).

Code-kentän arvon ollessaan 3, on kyseessä hylkäysviesti eli *Access-Reject*. Mikäli mikä tahansa attribuuteista ei täsmää, tulee RADIUS-palvelimen vaihtaa *Code*-kentän arvoksi 3. Kyseisessä tapahtumassa voi olla useampia vastausattribuutteja, jotka sisältävät mahdollisesti jonkinlaisen viestin jonka NAS-laite saattaa näyttää loppukäyttäjälle. *Identifier, Response Authenticator* sekä *Attributes*-kentät käyttäytyvät samalla tavalla kuin *Access-Accept*-viestissä (Rigney ym. 2013, 19).

Code-kentän arvon ollessa 4, on kyseessä lokitapahtuman aloittaminen eli *Accounting-Request*-viesti. Tällaisessa tapauksessa RADIUS-palvelin on määritelty olemaan *”Accounting Server”* eli palvelin, johon kirjataan ylös erilaisia verkkotapahtumia. Tällaisia tapahtumia voivat olla käyttäjän kirjautuminen verkkoon, järjestelmän uudelleenkäynnistäminen tai jotain muuta minkä verkon ylläpitäjät ovat määritelleet kirjattavaksi lokitapahtumaksi. Edellä esitetyistä tapahtumista lähetetään merkintä RADIUS-palvelimelle ja pakettiin merkitään *Code*-kentän arvoksi 4 (Rigney ym. 2013, 7).

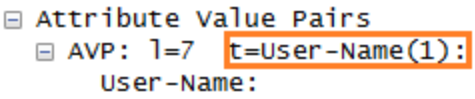
Onnistuneen tapahtuman kuittaamiseen RADIUS-palvelin lähettää viestin *Accounting-Response*, joka ilmoittaa että viesti on vastaanotettu ja kirjattu ylös onnistuneesti. Tällöin RADIUS-palvelin vaihtaa *Code*-kentän arvoksi 5. Prosessin aikana tapahtuessa jotain odottamatonta, RADIUS hylkää paketit hiljaisesti (Rigney ym. 2013, 8).

Mikäli RADIUS-palvelin on määritetty lähettämään loppukäyttäjälle haaste, on palvelimen vastattava *Access-Request*-viestiin vaihtamalla *Code*-kenttään arvo 11. Tässä tapauksessa on kyseessä *Access-Challenge*-viesti. *Identifier*, *Length* ja *Response Authenticator*-kentät toimivat samalla tavalla tässä kuin muissa *Access Request*-viestin vastauksissa, aivan kuten *Access-Ac*cept-viesteissä (Rigney ym. 2013, 21).

3.2.6 RADIUS attribuutit

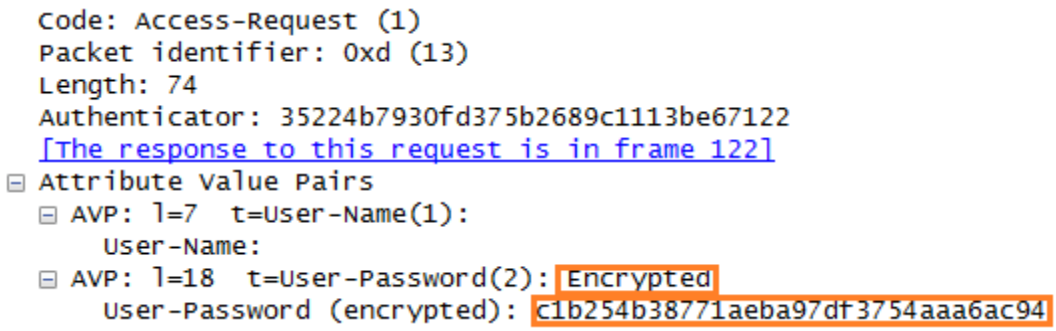
RADIUS-protokollan attribuutteja on paljon ja ne on listattu liitteeseen 1. Liitteessä 1 on esitetty missä viestissä mikäkin attribuutti esiintyy ja kuinka useasti.

User-Name-attribuutti sisältää käyttäjätunnuksen, jolla käyttäjä yrittää tunnistautua. *User-Name*-attribuutin tulee sisältyä *Access-Request*-viestiin. Käyttäjätunnuksen *Attributes*-kentän arvona on 1 ja sen pituus tulee olla vähintään 3 merkkiä. Käyttäjätunnuksen luomisessa on otettava huomioon, että RADIUS-attribuutti *User-Name* tukee ainoastaan UTF-8 koodausta, jonka on määritellyt kansainvälinen standardi ISO 10646 (Rigney ym. 2013, 25). Kuviossa 2 on esitelty Wireshark kuvakaappaus, jossa on attribuutti *User-Name* jonka arvo on 1.



KUVIO 2. RADIUS User-Name-attribuutti

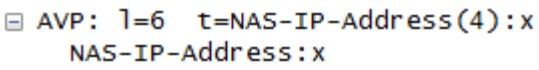
User-Password-attribuutti sisältää loppukäyttäjän salasanan, jota tämä käyttää autentikointiin. Kyseinen attribuutti lähetetään ainoastaan *Access-Request*-viestin yhteydessä ja se ei kulje verkossa selkokielisenä. Kuten aikaisemmin esitettiin, se on suojattu yksisuuntaisella *MD5*-algoritmilla (Rigney ym. 2013, 25). Kuviossa 3 on esitelty miltä RADIUS-protokollalla lähetetty salasana näyttää Wiresharkilla tarkasteltuna.



KUVIO 3. RADIUS-protokollan lähettämä salasana

NAS-IP-Address-attribuutti pitää sisällään NAS-laitteen IP-osoitteen, jonka kautta loppukäyttäjä yrittää kirjautua. Tämän IP-osoitteen pitäisi olla yksilöllinen ja etukäteen määritetty RADIUS-palvelimelle. NAS-laitteen IP-osoite attribuuttia käytetään ainoastaan *Access-Request*-viestissä, jotta RADIUS-palvelin pystyy varmentumaan siitä että loppukäyttäjä on luotettu henkilö ja hän yrittää kirjautua tunnetun laitteen

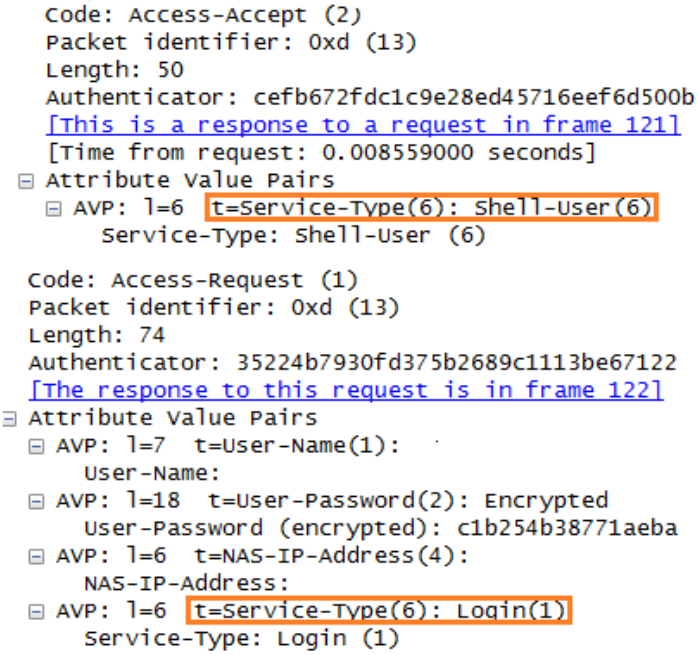
kautta (Rigney ym. 2013, 28). Kuviossa 4 on esitetty miltä *NAS-IP-Address*-attribuutti näyttää Wireshark kuvakaappauksessa. Huomattavaa on se, että IP-osoite kulkee selkokielisenä paketissa. IP-osoitteen selkokielinen esiintyminen paketissa ei ole hyvä asia. (Kuviosta on poistettu IP-osoite ja se on korvattu x:llä)



KUVIO 4. NAS-IP-Address Attribuutti

NAS-port-attribuutti ilmaisee fyysisen portin numeron, jonka takaa loppukäyttäjä yrittää autentikoida. Kyseinen attribuutti on käytössä ainoastaan *Access-Request*-viestissä. Kyseessä on fyysinen portti, ei TCP/UDP-portti (Rigney ym. 2013, 29).

Service-Type-attribuutti kertoo, minkälaista palvelua loppukäyttäjä haluaa tai minkälaista palvelua hänelle on tarjolla. Kyseistä attribuuttia käytetään mahdollisesti *Access-Request* ja *Access-Accept*-viesteissä (Rigney ym. 2013, 31–32). Kuviossa 5 on esitelty tapahtuma, jossa käyttäjä haluaa kirjautua laitteelle (Kuvion alaosassa) ja RADIUS tarjoaa tälle *Shell User*-palvelua (Kuvion yläosassa).

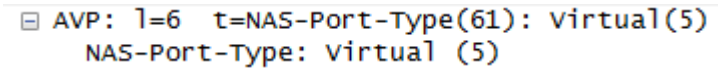


KUVIO 5. RADIUS service-type

Session-Timeout-attribuutti asettaa maksimiajan sekunteina siihen kuinka kauan palvelu on loppukäyttäjän käytössä ennen kuin istunto päätetään. Kyseistä attribuuttia voidaan käyttää joko *Access-Accept* tai *Access-Challenge*-viesteissä. *Idle-Timeout*-attribuutti asettaa ajan, jonka jälkeen istunto katkaistaan, mikäli loppukäyttäjä ei ole tehnyt mitään kyseisesen ajan kuluessa (Rigney ym. 2013, 48–49).

NAS-identifier-attribuutti sisältää merkkijonon, jonka perusteella NAS-laite voidaan tunnistaa. *Access-Request*-viestissä on oltava aina joko *NAS-IP-address* tai *NAS-identifier*-attribuutti (Rigney ym. 2013, 52).

NAS-Port-Type-attribuutin tehtävänä on kertoa portin tyyppi, jonka takaa loppukäyttäjä yrittää autentikoida. Taulukossa 2 on esitetty eri tyypit, joita loppukäyttäjä voi käyttää ja minkä *NAS-Port-Type*-attribuutti ilmoittaa (Rigney ym. 2013, 60). Kuviossa 6 on esitetty Wireshark kuvakaappaus tapahtumasta, jossa käyttäjä yrittää autentikoida itsensä verkkolaitteeseen, jolloin *NAS-Port-Type* attribuuttina on "*Virtual*", joka vastaa taulukon 2 arvoa 5.



KUVIO 6. NAS-Port-Type

TAULUKKO 2. NAS-Port-Type - attribuutin arvot

0	Async
1	Sync
2	ISDN Sync
3	ISDN Async V.120
4	ISDN Async V.110
5	Virtual
6	PIAFS
7	HDLC Clear Channel
8	X.25
9	X.75
10	G.3 Fax
11	SDSL - Symmetric DSL
12	ADSL - Asymmetric DSL
13	ADSL-DMS
14	IDSL - ISDN DSL
15	Ethernet
16	xDSL - unknown type of DSL
17	Cable
18	Wireless - Other
19	Wireless - IEEE 802.11

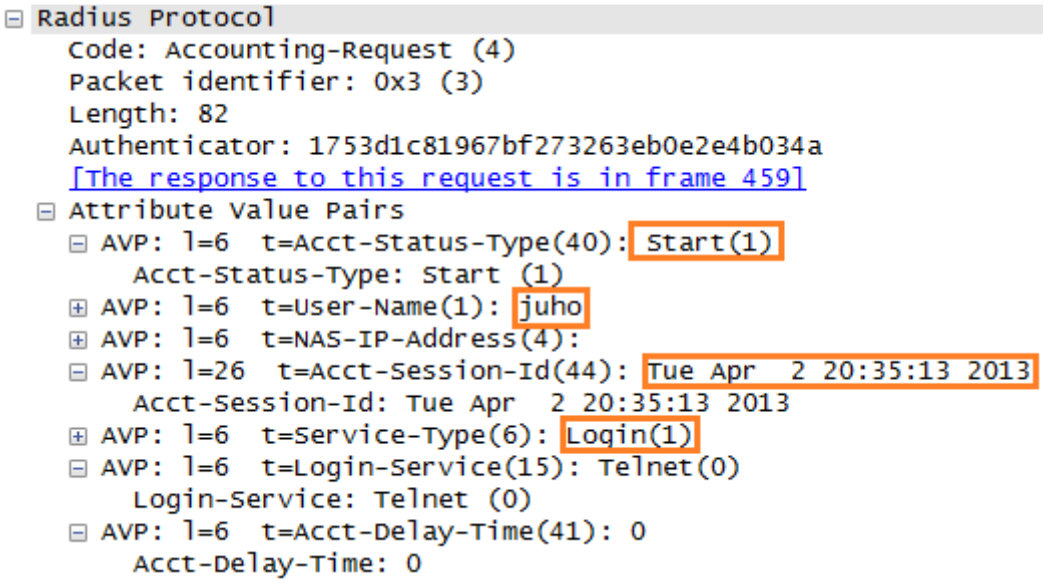
3.2.7 RADIUS-kirjanpito

RADIUS-kirjanpito (*Accounting*) on esitelty RFC-dokumentissa 2866. RFC:stä ilmenee, että RADIUS-kirjanpito-osuudessa käytetään ainoastaan kahta eri viestityyppiä, *Accounting-Request* ja *Accounting-Response*.

Perusidealtaan RADIUS-kirjanpito toimii niin, että loppukäyttäjän kirjauduttua laitteelle lähetetään määritetylle kirjanpitopalvelimelle tieto, että tiettyyn aikaan on tapahtunut istunnon aloittaminen. Istunnon loppuessa lähetetään lopetuksesta palvelimelle erikseen viesti. Kyseiset toiminnot voidaan määrittää laitteille käsin halutulla tavalla, esimerkiksi voidaan halutessa kerätä tietoa ainoastaan aloitetuista istunnoista.

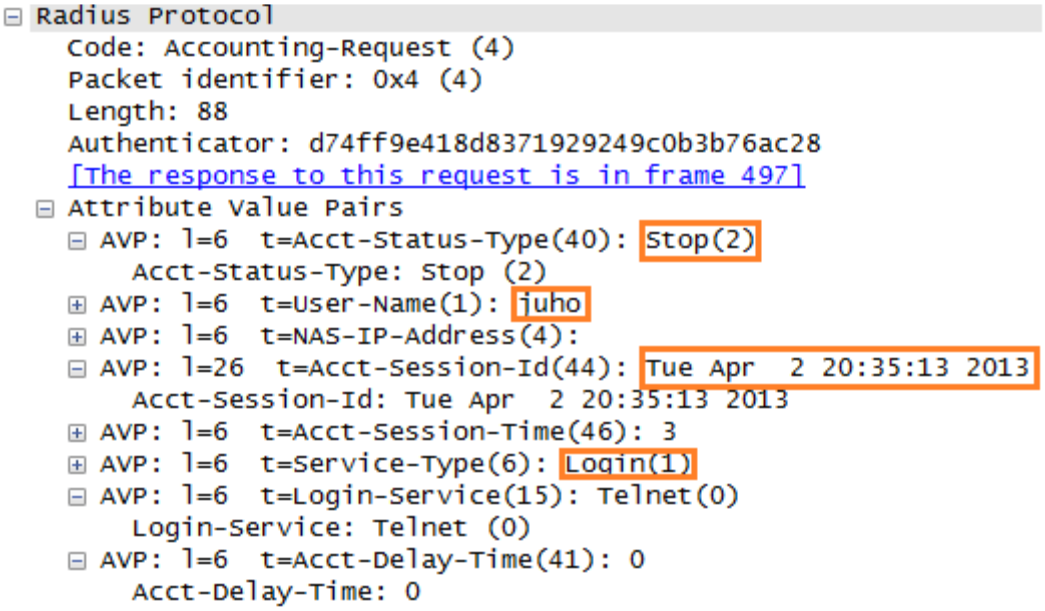
Kirjanpito-viestien lähettäminen ja niiden välittäminen useamman palvelimen tapauksessa tapahtuu vastaavasti kuin autentikointi osuudessa (Rigney Livinstong 2013, 3).

Accounting-Request-viesti lähetetään kirjanpitopalvelimelle asiaakkalta, joka on pääasiassa NAS-laite. *Accounting-Request*-viesteissä *code*-kentän arvoksi asetetaan 4. Jokaiseen *Accounting-Request*-viestiin tulee aina kuittaus kun viesti on onnistuneesti kirjattu ylös. Onnistuneissa kirjauksissa *Code*-kentän arvo on 5. Vika tilanteissa viestiin ei tule mitään vastausta. Kaikki pätevät attribuutit, joita käytetään *Access-Request* tai *Access-Accept*-viesteissä, ovat päteviä myös kirjanpito-osuudessa. Muutamia attribuutteja ei kuitenkaan saa esiintyä *Accounting*-viesteissä, kuten käyttäjän salasana. RADIUS-kirjanpitopaketin rakenne on samanlainen kuin normaali RADIUS-paketti (Rigney Livinstong, 2013, 7). Kuviossa 7 ja 8 on esitelty Wireshark kuvakaappaus tapahtumasta, jossa käyttäjä *Juho* on autentikoitunut laitteelle ja lopettanut istunnon (Start & Stop).



KUVIO 7. RADIUS–kirjanpito start-viesti

Seuraavaksi on esitelty lopetusviesti kuviossa 8.



KUVIO 8. RADIUS–kirjanpito stop-viesti

Kirjanpitoviesteihin voidaan asettaa taulukon 3 mukaisia asioita ja suuri määrä muita attribuutteja, jotka eivät ole tämän opinnäytteen kannalta relevantteja.

TAULUKKO 3. Kirjanpitoattribuutteja

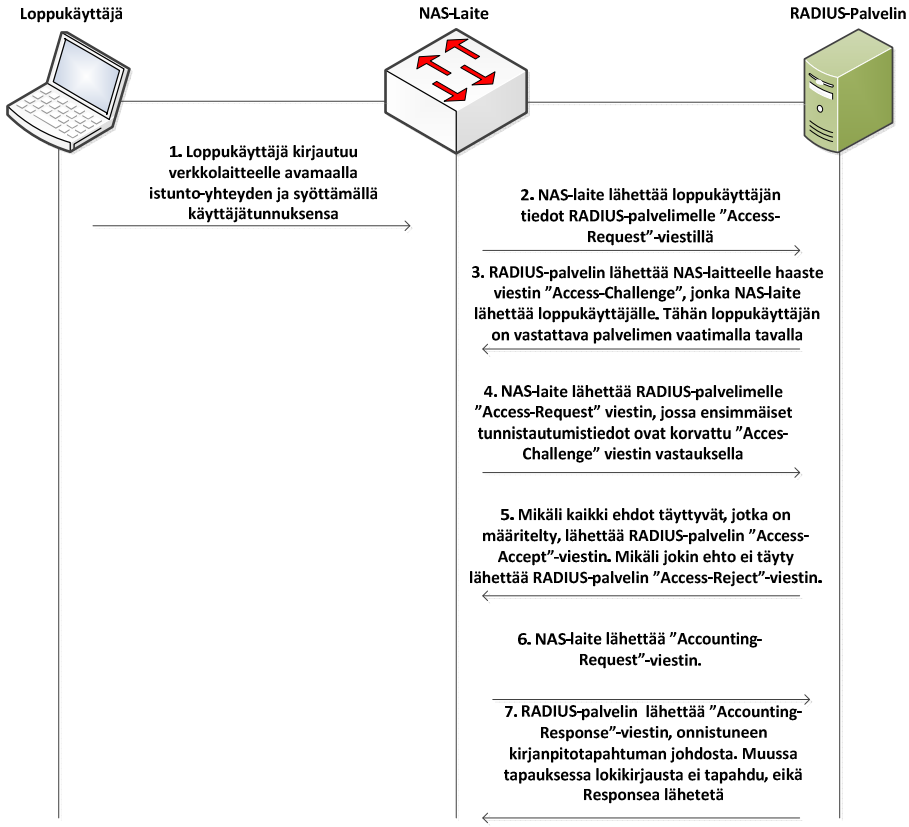
Attribuutti	**Selite**
Status-type	2 arvoa, aloitus ja lopetus, jotka voidaan lokittaa
Delay-time	Aika, joka kuluu kirjanpitoviestin lähettämiseen
Session-id	Uniikki numero, joka on sama aloitus ja lopetusviesteillä
Authentic	Kirjanpito käyttäjien tunnistautumisesta
Session-Time	Käyttäjän istunnon ajan pituus
NAS-IP-address	NAS -laitteen IP-osoite
Service type	Palvelun tyyppi
Login service	Millä kirjaudutaan sisään

Attribuutteja on RADIUS-protokollalla lukuisia. Seuraavassa kuviossa 9 on Wireshark kuvakaappaus muutamista kirjausattribuuteista, niin lähetys kuin kuittausviestien yhteydessä (Request & Response). Huomio kuitenkin kiinnittyi siihen, että RADIUS ei mahdollista syötettyjen komentojen kirjanpitoa.

```
Attribute Value Pairs
  AVP: l=6  t=Acct-Status-Type(40): Start(1)
  AVP: l=6  t=User-Name(1): juho
  AVP: l=6  t=NAS-IP-Address(4):
  AVP: l=26  t=Acct-Session-Id(44):20:35:13 2013
  AVP: l=6  t=Service-Type(6): Login(1)
  AVP: l=6  t=Login-Service(15): Telnet(0)
  AVP: l=6  t=Acct-Delay-Time(41): 0
Attribute Value Pairs
  AVP: l=6  t=Acct-Status-Type(40): Stop(2)
  AVP: l=6  t=User-Name(1): juho
  AVP: l=6  t=NAS-IP-Address(4):
  AVP: l=26  t=Acct-Session-Id(44):20:35:13 2013
  AVP: l=6  t=Acct-Session-Time(46): 3
      Acct-Session-Time: 3
  AVP: l=6  t=Service-Type(6): Login(1)
  AVP: l=6  t=Login-Service(15): Telnet(0)
  AVP: l=6  t=Acct-Delay-Time(41): 0
```

KUVIO 9. RADIUS-kirjanpito

Yhteenvetona kuviossa 10 on esitelty perustilanne liikennöinnistä kun RADIUS-palvelin on käytössä. Kuviossa tapahtumat 1 - 5 ovat pakollisia ja tapahtumat 6 – 7 ovat vaihtoehtoisia tapahtumia liittyen kirjanpitoon.



KUVIO 10. RADIUS-viestien lähettäminen

3.3 Terminal Access Controller Access Control System

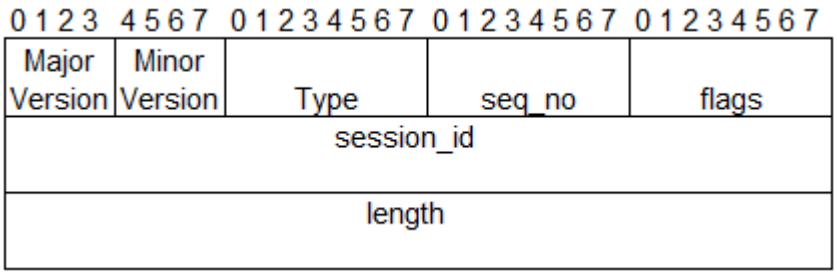
Terminal Access Controller Access Control System (TACACS) on Cisco Systemsin kehittämä protokolla. TACACS tarjoaa AAA-arkkitehtuurin mukaisen kokonaisuuden, jonka avulla voidaan erottaa autentikointi, valtuuttaminen ja lokitietojen kerääminen. TACACS toimii RADIUS-protokollan mukaan asiakas-palvelin-mallin mukaisesti. TACACS-protokollasta on kehitetty uudempi versio TACACS+, joka on nykyään yleisemmin käytössä ja näin ollen tässä opinnäytetyössä perehdytään syvemmin TACACS+ ja RADIUS-protkollien eroavaisuuksiin (Bhaiji 2013).

Cisco Systemsin omat laitteet tukevat lähes poikkeuksetta TACACS+-protokollaa. TACACS-protokolla on esitelty *”draft-grant-tacacs-2.txt”*-dokumentissa (Bhaiji 2013).

3.3.1 TACACS+

TACACS+-protokolla salaa kaiken AAA-liikenteen NAS-laitteen ja TACACS+-palvelimen välillä, toisin kuin RADIUS joka salaa ainoastaan salasanan. TACACS+ on joustava protokolla siinä mielessä, että se mahdollistaa lähes minkä tahansa autentikointi menetelmän. TACACS+-protokolla käyttää kuljetusprotokollanaan TCP:tä, joka varmistaa pakettien perille menon (Carrel & Grant 2013, 4).

TACACS+-paketin otsake on aina selväkielinen ja siinä esitellään käytettävissä oleva *versio*, *tyyppi*, *sekvenssinumero*, *liput*, istunnon *järjestysnumero* ja paketin *pituus*. Paketti on 12 tavun mittainen. Kuviossa 11 on esitelty TACACS+-paketin otsake (Carrel & Grant 2013, 4).



KUVIO 11. TACACS+-paketin otsake

Major version on TACACS version numero, joka on TACACS+ tapauksessa:

TAC_PLUS_MAJOR_VER := 0xc

*Minor Version*in tarkoituksena on mahdollistaa TACACS+-protokollan yhteensopivuus vanhempien versioiden kanssa. *Major* ja *Minor*-version-kentät ovat molemmat tavun mittaisia (Carrel & Grant 2013, 4).

Type-kenttä on pituudeltaan yhden tavun ja kyseisessä kentässä määritellään mitä AAA-arkkitehtuurin osa-aluetta käytetään. Kuviossa 12 on esitetty minkä *Type*-arvon otsake saa missäkin tapauksessa (Carrel & Grant 2013, 5).

TAC_PLUS_AUTHEN := 0x01	Authentication
TAC_PLUS_AUTHOR := 0x02	Authorization
TAC_PLUS_ACCT := 0x03	Accounting

KUVIO 12. Type-kentän arvot ja merkitykset

Seq_no-kentän pituus on *Type*-kentän tapaan yksi tavu. Kyseisen kentän tehtävänä on määrätä sekvenssinumero tietylle paketille ja istunnolle. Toisin sanoen ensimmäisen paketin arvo on yksi ja aina kun uutta pakettia lähetetään, kasvatetaan *seq_no*-arvoa yhdellä. Tästä seuraa se, että TACACS+-asiakkaat lähettävät ainoastaan paketteja jotka sisältävät parittoman sekvenssinumeron ja TACACS+-palvelin lähettää paketteja joissa sekvenssinumero on parillinen. *Seq_no*-kentän arvo ei saa koskaan ylittää arvoa $2^{(8)}$-1 eli arvoa 255. Mikäli kyseinen arvo saavutetaan, täytyy istunto keskeyttää ja aloittaa uudelleen, jolloin sekvenssinumerointi alkaa alusta (Carrel & Grant 2013, 5).

Flags-kenttä on yhden tavun mittainen. Tämän kentän tarkoituksena on kertoa, että onko yhteys salattua vai ei. Mikäli *Flags*-kentän arvona on 0x01 eli *TAC_PLUS_UNENCRYPTED_FLAG,* on viesti salaamatonta. Mikäli lippua ei aseteta, on viesti oletuksena salattu. Salaamattomia viestejä ei kuitenkaan kannata käyttää normaalissa käytössä. Testiympäristöissä voidaan tutkimus mielessä asettaa lippuarvoksi 0x01. Lipun arvon ollessa 0x04 on kyseessä *TAC_PLUS_SINGLE_CONNECT_FLAG* eli kyseessä on TCP-kanavointiin liittyvä lippuarvo. NAS-laitteen asettaessa lipulle tämän

arvon kertoo se, että se voi käsitellä useampaa kuin yhtä TACACS+-istuntoa yhden TCP-yhteyden yli (Carrel & Grant 2013, 6).

Session_ID-kenttä on pituudeltaan 4 tavua ja kertoo tunnuksen kyseiselle TACACS+-istunnolle. Tunnus on täysin sattumanvaraisesti arvottu ja se ei muutu koko TACACS+-istunnon aikana. Mikäli kyseinen tunnus ei olisi tietoturvallisesti vahva, se heikentäisi TACACS+-protokollan tietoturvaa (Carrel & Grant 2013, 6).

Viimeisenä TACACS+-otsakkeesta löytyy *Length*-kenttä, jonka pituus on 4 tavua. Kyseinen kenttä kertoo koko TACACS+-paketin pituuden, lukuun ottamatta otsakkeen pituutta, sillä se on aina 12-tavua (Carrel & Grant 2013, 6).

3.3.2 TACACS+-kenttien salaus

TACACS+-paketti suojataan vain yhdellä salausmekanismilla istuntoa kohden. Paketille generoidaan suojaus ketjuttamalla sarja *MD5*-tiivisteitä, joista jokainen on 16-tavun mittainen. Edellä esitetty ketjutus tehdään vaiheittain. Istunnon tunnus, jaettu salaisuus, versionumero ja sekvenssinumero on generoitu ensimmäiseen *MD5*-tiivisteeseen. Tämän jälkeen *MD5*-tiiviste ajetaan vielä tämän generoidun tiivisteen yli. Edellä mainituista arvoista kaikki sijaitsevat paketin otsakkeessa paitsi jaettu salaisuus, jota käytetään palvelimen ja asiakkaan väliseen tunnistautumiseen. *MD5*-tiiviste sarjat siis toimivat seuraavalla tavalla: (Carrel & Grant 2013, 8-9)

MD5_tiiviste1 = MD5{Sessio ID, Avain, Versio, Sekvenssi no}

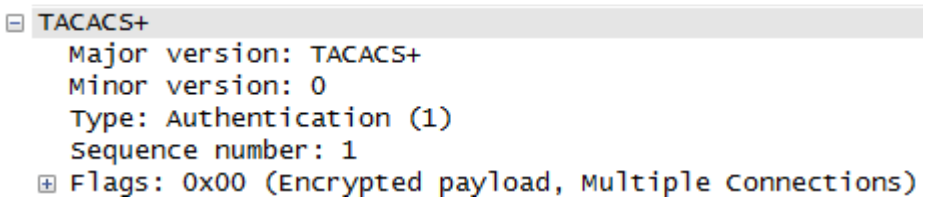
MD5_tiiviste2 = MD5{Sessio ID, Avain, Versio, Sekvenssi no, MD5_tiiviste1}

MD5_tiivisteX = MD5{Sessio ID, Avain, Versio, Sekvenssi no, MD_tiivisteX – 1}

3.3.3 TACACS+ Autentikaatio

TACACS+-autentikaatiossa on käytössä kolme eri viestityyppiä: *START*, *CONTINUE* ja *REPLY*. *START* ja *CONTINUE*-viestit ovat viestejä joita NAS-laite lähettää. *REPLY*-viestit saapuvat aina palvelimelta NAS-laitteelle. Autentikaatioprosessi alkaa siitä kun NAS-laite lähettää palvelimelle *START*-viestin, joka sisältää käytössä olevan autentikaatiotavan. Se voi myös sisältää käyttäjätunnuksen ja jotakin autentikaatiodataa kuten

salasanan. *START*-viesti aloittaa aina TACACS+-autentikaatioprosessin ja näin ollen *seq_no* -arvo on 1 (Carrel & Grant 2013, 9). Kuviossa 13 on NAS-laitteen lähettämä ensimmäinen autentikaatio-viesti.



KUVIO 13. TACACS START-viesti

START-viestiin vastauksena palvelin lähettää *REPLY*-viestin, joka ilmoittaa onko autentikaatio valmis vai odottaako palvelin vielä jotain muuta tunnistetietoa. Mikäli palvelimen lähettämä vastaus osoittaa, että autentikaatioprosessia tulee jatkaa, niin on NAS-laitteen vastattava tähän *CONTINUE*-viestillä. Palvelimen tulee aina vastata viesteihin *REPLY*-viestillä. Poikkeuksena on keskeytys, josta NAS-laite ilmoittaa. Tällaisissa tapauksissa istunto on pysäytettävä välittömästi (Carrel & Grant 2013, 9). Autentikaation *START*-viestin runko on esitelty kuviossa 14.

1 2 3 4 5 6 7 8	1 2 3 4 5 6 7 8	1 2 3 4 5 6 7 8	1 2 3 4 5 6 7 8
Action	Priv_lvl	Authen_type	Service
user len	port len	rem_addr len	data len
user …			
port …			
rem_addr …			
data …			

KUVIO 14. START-viestin runko

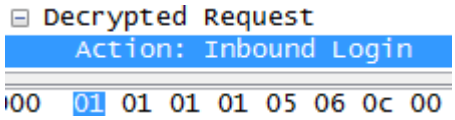
START-viestin runkoa tarkastellessa voidaan huomata, että *Action*, *Priv_lvl*, *Authen_type*, *Service*, *User len*, *Port len*, *Rem_addr len* ja *Data len*-kentät ovat yhden tavun mittaisia ja loput kentät ovat neljän tavun mittaisia.

Action-kenttä ilmaisee, että minkälainen toiminto on kyseessä. Sallitut arvot ovat esitelty kuviossa 15 (Carrel & Grant 2013, 10).

TAC_PLUS_AUTHEN_LOGIN	:= 0x01
TAC_PLUS_AUTHEN_CHPASS	:= 0x02
TAC_PLUS_AUTHEN_SENDPASS	:= 0x03
TAC_PLUS_AUTHEN_SENDAUTH	:= 0x04

KUVIO 15. Action-kentän arvot ja merkitykset

Action-kenttää tarkastellessa huomataan kuvion 16 osoittamalla tavalla, että kyseinen kenttä toimii protokollakuvauksen mukaisesti.



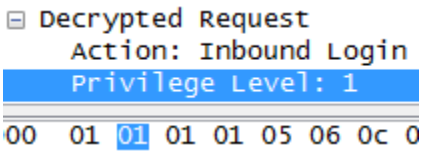
KUVIO 16. Action–kenttä arvo 0 = login

Priv_lvl-kenttä kertoo minkä tasoinen käyttäjä on autentikoitunut. *Privilege*-oikeuksia voidaan myöntää arvojen 0 ja 15 välillä. Mitä pienempi arvo on, sitä vähemmän on käytettäviä oikeuksia oletuksena. Oletuksena on asetettu eri arvoja, jotka on esitelty kuviossa 17. Arvo *0x0f* eli desimaaliarvo 15 kertoo, että käyttäjällä on täydet oikeudet (privilege 15) (Carrel & Grant 2013, 11).

TAC_PLUS_PRIV_LVL_MAX	:= 0x0f
TAC_PLUS_PRIV_LVL_ROOT	:= 0x0F
TAC_PLUS_PRIV_LVL_USER	:= 0x01
TAC_PLUS_PRIV_LVL_MIN	:= 0x00

KUVIO 17. Priv_lvl arvot ja merkitykset oletuksena

Privilege-kenttää tutkiessa huomataan myös, että arvot vastaavat kuviossa 18 TACACS+-dokumentin arvoja kuten kuviossa 18 on esitetty Wireshark kuvakaappauksen avulla.



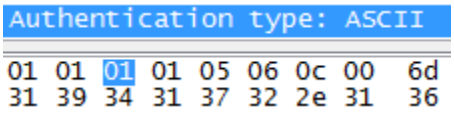
KUVIO 18. Privilege Level-kenttä

Authen_type-kenttä ilmaisee autentikoinnin tyypin, jota käytetään autentikoinnissa. Kuviossa 19 on esitetty eri tyypit ja niiden arvot (Carrel & Grant 2013, 12).

```
TAC_PLUS_AUTHEN_TYPE_ASCII  := 0x01
TAC_PLUS_AUTHEN_TYPE_PAP    := 0x02
TAC_PLUS_AUTHEN_TYPE_CHAP   := 0x03
TAC_PLUS_AUTHEN_TYPE_ARAP   := 0x04
```

KUVIO 19. Authen_type arvot ja merkitykset

Authentication Type-kentästä voidaan havaita, että kyseisen kentän arvot ovat paikkaansa pitäviä kuvion 20 osoittamalla tavalla.



KUVIO 20. AuthType-kenttä

Service-kenttä ilmaisee palvelun, joka on pyytänyt autentikaatiota. Kuviossa 21 on esitelty *Service*-kentän arvot ja merkitykset (Carrel & Grant, 2013, 12).

```
TAC_PLUS_AUTHEN_SVC_NONE        := 0x00
TAC_PLUS_AUTHEN_SVC_LOGIN       := 0x01
TAC_PLUS_AUTHEN_SVC_ENABLE      := 0x03
TAC_PLUS_AUTHEN_SVC_PPP         := 0x04
TAC_PLUS_AUTHEN_SVC_ARAP        := 0x06
TAC_PLUS_AUTHEN_SVC_RCMD        := 0x07
TAC_PLUS_AUTHEN_SVC_x25         := 0x08
TAC_PLUS_AUTHEN_SVC_FWPORXY     := 0x09
```

KUVIO 21. Service-kentän arvot ja merkitykset

Kuviossa 22 huomataan *Service*-kentän paikkansapitävyys.

```
Service: Login
01 01 01 01 05 06
31 39 34 31 37 32
```

KUVIO 22. Service–kenttä

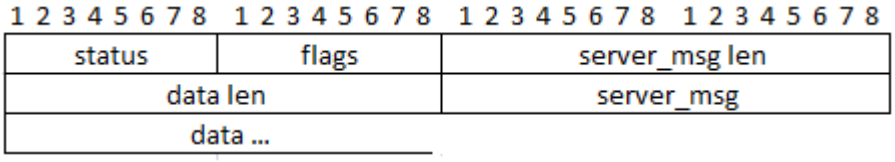
User-kenttä on valinnainen tässä paketissa, mutta sen avulla voidaan ilmaista nimensä mukaisesti käyttäjän syöttämä merkkijono. Kyseisessä kentässä kulkee myös käyttäjän syöttämä salasana, jota käytetään autentikoitumiseen TACACS+-palvelimelle. *User len*-kentän tarkoituksena on kertoa *User*-kentän pituus (Carrel & Grant 2013, 12).

Port-kentän tehtävänä on ilmaista portti, jonka takana autentikoitava käyttäjä sijaitsee. *Rem_addr*-kentän tarkoituksena on kertoa käyttäjän sijainti. Kyseessä on valinnainen kenttä, koska tietoa ei ole välttämättä aina saatavilla (Carrel & Grant 2013, 13). Kuviossa 23 on esitetty *Port* ja *Rem_addr*–kenttien näkymät.

```
Port: tty194
Remaddr len:
Remote Address:
Data: 0 (not used)
01 01 01 01 05 06 0c 00  6d 79
31 39 34 31 37 32 2e 31  36 2e
```

KUVIO 23. Port ja Rem_add-kentät

TACACS+-palvelin lähettää vain yhdenlaisia paketteja NAS-laitteelle liittyen autentikaatioon. Kyseessä on *Authentication Reply*-viesti, jonka rakenne on kuvattu kuviossa 24 (Carrel & Grant 2013, 14).



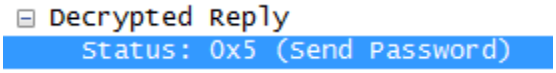
KUVIO 24. Authentication Reply

Status-kentän tehtävänä on kertoa vastauksen tila eli onko kyseessä esimerkiksi viesti jolla hyväksytään autentikaatio, vai pyydetäänkö jotain tietoja lisää. Kuviossa 25 on esitelty erilaiset *Status*-kentän-tilat *Authentication Reply*-viestissä (Carrel & Grant 2013, 14).

TAC_PLUS_AUTHEN_STATUS_PASS	:= 0x01
TAC_PLUS_AUTHEN_STATUS_FAIL	:= 0x02
TAC_PLUS_AUTHEN_STATUS_GETDATA	:= 0x03
TAC_PLUS_AUTHEN_STATUS_GETUSER	:= 0x04
TAC_PLUS_AUTHEN_STATUS_GETPASS	:= 0x05
TAC_PLUS_AUTHEN_STATUS_RESTART	:= 0x06
TAC_PLUS_AUTHEN_STATUS_ERROR	:=0x07
TAC_PLUS_AUTHEN_STATUS_FOLLOW	:= 0x021

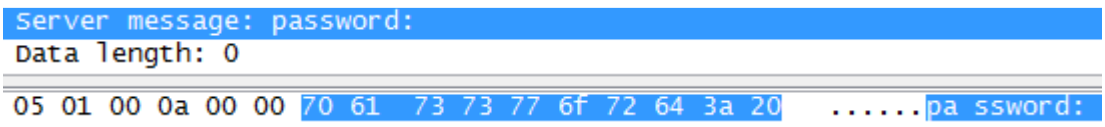
KUVIO 25. Authentication Reply statusarvot

Käyttäjän syötettyään NAS-laitteelle käyttäjätunnuksen, pyytää TACACS+-palvelin usein lisätietoja autentikaatiota varten, kuten kuviossa 26 on pyydetty salasanaa.



KUVIO 26. Reply arvo 0x5

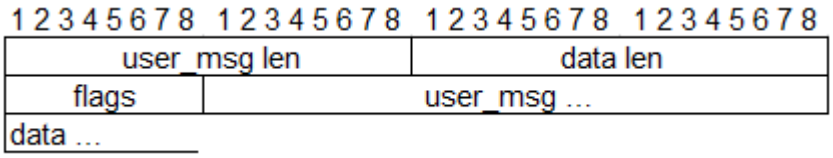
Server_msg-kenttä on valinnainen. Mikäli se on käytössä, se esitetään aina loppukäyttäjälle. *Server_msg*-viesti voidaan näyttää esimerkiksi sen takia, että TACACS+-palvelin haluaa käyttäjän syöttävän salasanansa. Kuviossa 27 on esitetty *Server_msg*-viesti *”password:”* (Carrel & Grant 2013, 15).



KUVIO 27. Srv_msg-viesti ’password:’

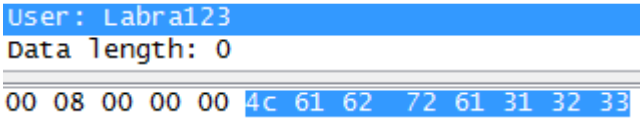
Data-kenttä sisältää dataa, joka on osa autentikaatiprosessia ja se on tarkoitettu ainoastaan NAS-laitteelle, ei loppukäyttäjälle (Carrel & Grant 2013, 15).

Seuraavassa kuviossa 28 on esitelty *Authentication CONTINUE* paketin rakenne. Kyseinen paketti kulkee aina NAS-laitteelta palvelimelle ja se lähetetään *Reply*-viestin jälkeen. (Carrel & Grant 2013, 15)



KUVIO 28. TACACS Auth continue-paketin rakenne

User_msg-kenttä osoittaa merkkijonon jonka loppukäyttäjä on syöttänyt vastauksekssi *Srv_msg*-viestiin (Carrel & Grant 2013, 15). Kuviossa 29 on käyttäjän syöttämä *"Labra123" User_msg*–viesti.



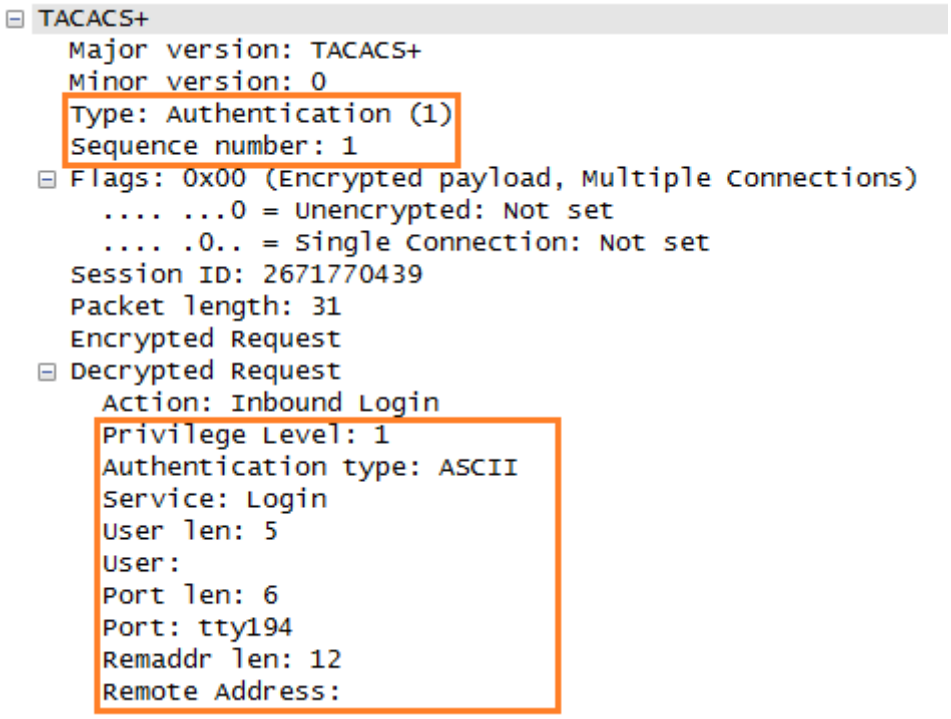
KUVIO 29. User_msg-viesti

3.3.4 TACACS+ autentikaatioprosessi

Autentikaatioprosessi toimii lyhyesti sillä tavalla, että NAS-laite lähettää autentikaatio aloitusviestissä seuraavia tietoja:

- Privilege–taso
- Palvelutieto
- Porttitieto
- Osoitetieto

Continue-viesteissä kyseisiä tietoja lähetetään *User_msg*-kentässä, jotka ovat usein vastauksia palvelimelta tulleisiin *Srv_msg*-viesteihin (Carrel & Grant 2013, 16). Kuviossa 30 on esitetty TACACS+-viesti, jonka sekvenssinumero on 1 eli kyseessä on autentikaation aloittava viesti.



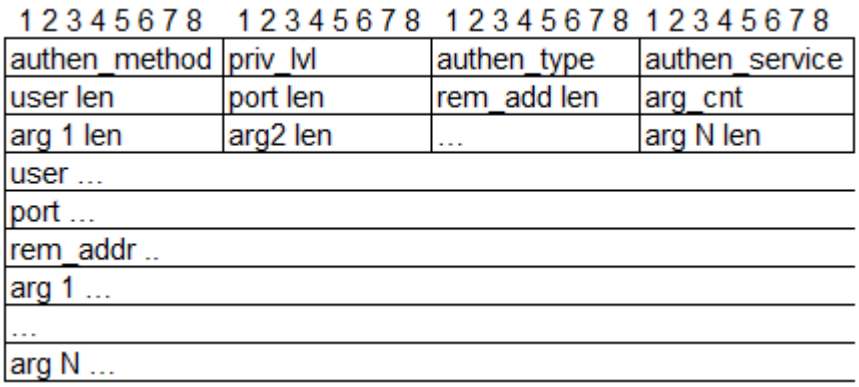
KUVIO 30. TACACS autentikointiprosessin aloitusviesti

Tähän viestiin palvelin vastaa normaalisti pyytämällä lisätietoja, kuten salasanaa tai vaihtoehtoisesti terminoi istunnon hylkäämällä tai hyväksymällä sen. Mikäli vastausviesti sisältää jonkinlaisen vastausviestin (*GETDATA/USER/PASS*), niin loppukäyttäjälle esitetään komentorivillä viesti, jossa palvelin pyytää jotain tietoa edellä mainituista tiedoista. Tämän jälkeen NAS-laitteen on pakko välittää viesti palvelimelle *User_msg*-viestissä (Carrel & Grant 2013, 16).

3.3.5 TACACS+ valtuutus

Toisin kuin RADIUS TACACS+ luo oman prosessinsa valtuuttamista varten, joka koostuu kahdesta erilaisesta viestistä: *REQUEST* ja *RESPONSE*-viestit. Valtuutuspyyntöviesti koostuu tiedoista joita on käytetty autentikoinnissa tai erikseen määritellyistä argumenteista. Vastaus-viesti sisältää vaihtelevan joukon argumentteja, joilla voidaan rajoittaa loppukäyttäjän toiminteita (Carrel & Grant 2013, 24).

Valtuutuspaketin rakenne on esitelty kuviossa 31.



KUVIO 31. TACACS+-valtuutuspaketti

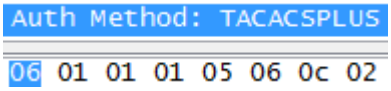
Ensimmäisenä paketissa on *Authen_method* joka nimensä mukaisesti ilmaisee autentikointiin käytettävän metodin. Metodit on esitelty taulukossa 4 (Carrel & Grant 2013, 25).

TAULUKKO 4. TACACS+ Valtuutus authe_meth paketin arvot

TAC_PLUS_AUTHEN_METH_NOT_SET	:= 0x00
TAC_PLUS_AUTHEN_METH_NONE	:= 0x01
TAC_PLUS_AUTHEN_METH_KRB5	:= 0x02
TAC_PLUS_AUTHEN_METH_LINE	:= 0x03
TAC_PLUS_AUTHEN_METH_ENABLE	:= 0x04
TAC_PLUS_AUTHEN_METH_LOCAL	:= 0x05
TAC_PLUS_AUTHEN_METH_TACACSPLUS	:= 0x06
TAC_PLUS_AUTHEN_METH_GUEST	:= 0x08
TAC_PLUS_AUTHEN_METH_RADIUS	:= 0x10
TAC_PLUS_AUTHEN_METH_KRB4	:= 0x11
TAC_PLUS_AUTHEN_METH_RCMD	:= 0x20

KRB4 ja *KRB5* ovat eri versioita kerberos-protokollasta. *Line* kertoo, että kyseessä on kiinteä salasana jolla käyttäjä kirjautuu. *Local* kertoo, että kyseessä on NAS-laitteen paikallinen käyttäjätietokanta johon autentikaatio perustuu. *Enable* on komento jolla autentikoidaan uudelle privilege tasolle. *TACACSPLUS* ja *RADIUS* ovat nimensä mukaisesti TACACS+ ja RADIUS- protokollat (Carrel & Grant 2013, 26).

Kuviossa 32 on esitetty TACACS+-valtuutuspaketti, jossa A*uth_meth* on saanut arvon 06, eli ”*TACACSPLUS*”.



KUVIO 32. Auth_Method TACACSPLUS/06

Valtuutuspyynnön paketin perusrakenteessa kaikki kentät ovat melko selkeitä ja nimistä pääteltäviä. Valtuutuksen argumentit ovat molemmissa viestityypeissä attribuuttiarvopareja. *Priv_lvl* kertoo nimensä mukaisesti käyttäjän nykyisestä *privilege*-tasosta. Authen_type kertoo autentikaatiotavasta joka suoritetaan. *Authen_service* kertoo palvelun, jota käyttäjä haluaa käyttää. User, Port ja Rem_addr–kenttien tarkoitus ei ole muuttunut. Seuraavana vuorossa on *Arg_count* jonka tehtävänä on ilmaista, että kuinka monta valinnaista argumenttia paketti sisältää (Carrel & Grant 2013, 27). Kuviossa 33 on esitelty arvopareja, sekä kuviossa on havaittavissa edellä kappaleessa esitetyt kentät.

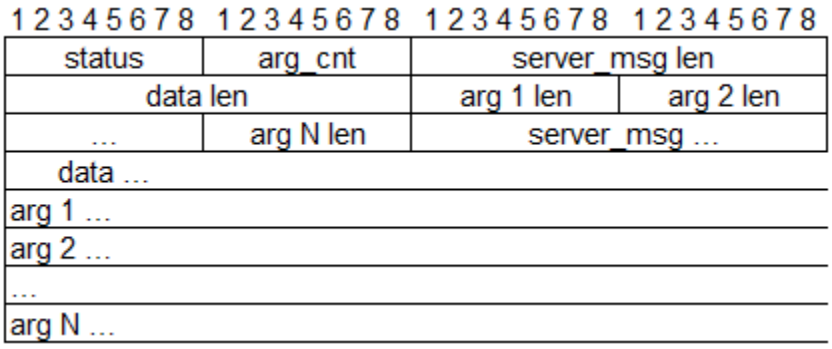
```
Privilege Level: 1
Authentication type: ASCII
Service: Login
User len:
User:
Port len: 6
Port: tty194
Remaddr len:
Remote Address:
Arg count: 2
Arg[0] length: 13
Arg[0] value: service=shell
Arg[1] length: 4
Arg[1] value: cmd*
```

KUVIO 33. Valtuutuspaketin sisältö

Edellä olevasta kuviosta voidaan havaita, että käyttäjän nykyinen privilege-taso on 1, autentikaatiotapa on ASCII ja palvelu jota käyttäjä pyytää on kirjautuminen laitteelle. Käyttäjä, portti ja osoite ovat samoja kuin aikaisemmin esitettiin. Seuraavana on *Arg* count eli kenttä joka ilmoittaa kuinka monta argumenttia paketissa on käytössä.

Tässä tapauksessa argumentteja on 2: Palveluksi on määritetty *shell* (=) ja komentoja (cmd*) ei ole rajattu.

Seuraavassa kuviossa 34 on esitelty TACACS+ -valtuutuspaketin vastausviesti.



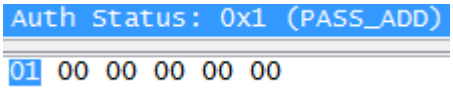
KUVIO 34. Valtuutuksen vastausviesti

Seuraavassa taulukossa 5 on esitetty *status*-kentän arvot ja niiden merkitykset.

TAULUKKO 5. Valtuuttamisviestin vastausarvot

TAC_PLUS_AUTHOR_STATUS_PASS_ADD	:= 0x01
TAC_PLUS_AUTHOR_STATUS_PASS_REPL	:= 0x02
TAC_PLUS_AUTHOR_STATUS_FAIL	:= 0x10
TAC_PLUS_AUTHOR_STATUS_ERROR	:= 0x11
TAC_PLUS_AUTHOR_STATUS_FOLLOW	:= 0x21

Status-kenttä yksinkertaisuudessaan kertoo, että onko valtuuttaminen mennyt läpi tai onko siinä tapahtunut virheitä (Carrel & Grant 2013, 31). Kuviossa 35 on esitetty viesti, jossa TACACS+-palvelin on lähettänyt onnistuneesta valtuuttamisesta kuittauksen.



KUVIO 35. Kuittaus onnistuneesta valtuuttamisesta

Server_msg-kenttä ilmaisee palvelimen lähettämän viestin käyttäjälle, mikäli palvelin sellaisen lähettää. *Data*-viesti pitää sisällään *ASCII* -koodatun merkkijonon, joka voidaan näyttää tai lokittaa. *Arg_cnt*-kenttä ajaa samaa asiaa kuin mitä valtuuttamisen pyynnössä, aivan kuten *Arg*-kentät muutenkin. *Arg*-kenttä on vastausviestissä sidon-

nainen pääosin *Status*-kenttään. Mikäli *status* saa arvon 1, valtuutus on onnistunut käyttäjän ehdottamin argumentein, jolloin vastausviestissä *Arg_cnt*-kentän arvo on 0. Arvon ollessa 2 on palvelin korvannut pyynnössä olleet argumentit omilla argumenteilla, joita palvelin voi tarjota kyseiselle käyttäjälle. Arvon ollessa 10 valtuutus on epäonnistunut. Arvon ollessa 11 palvelin ilmaisee, että valtuuttamisessa on tapahtunut jonkinlainen virhe. Virheen tapahtuessa millään argumenttiarvolla ei ole enää merkitystä. Viimeinen arvo tälle on 21 jolloin kyseessä on viesti, jossa toimenpiteet sijaitsevat *data*-kentässä ja *Arg_cnt-kentän* arvo on 0 (Carrel & Grant 2013, 32).

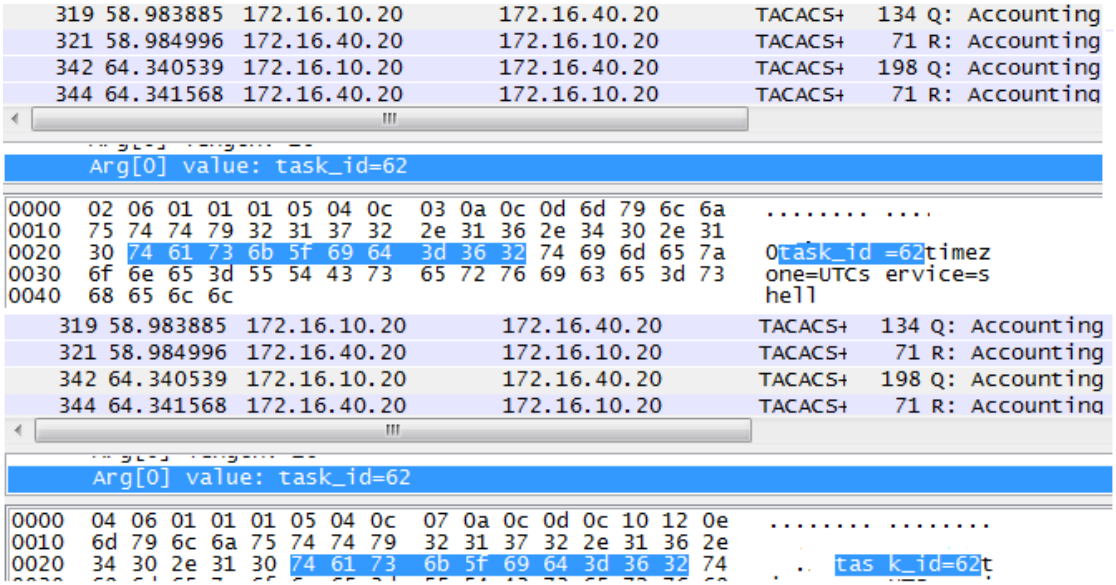
3.3.6 TACACS+-kirjanpito

TACACS+-kirjanpito toimii pääosin samalla tavalla kuin valtuuttaminen ja pakettien rakenne on samankaltainen kuin valtuuttamisessa. Kuviossa 36 on esitetty kirjanpitoon tarkoitettu TACACS+-paketti. Kirjanpito osio pitää sisällään kaikki samat attribuuttiarvoparit kuin valtuuttaminen, muutamia lisäyksiä lukuunottamatta (Carrel & Grant 2013, 33).

1 2 3 4 5 6 7 8	1 2 3 4 5 6 7 8	1 2 3 4 5 6 7 8	1 2 3 4 5 6 7 8
flags	authen_meth	priv_lvl	authen_type
authen_serv	user len	port len	rem_addr len
arg_cnt	arg1 len	arg 2len	…
arg N len	user …		
port …			
rem_addr …			
arg 1…			
…			
arg N …			

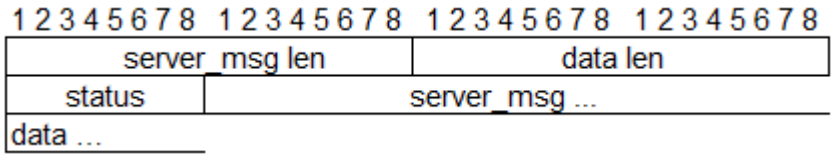
KUVIO 36. TACACS+-kirjanpitopaketti

Flags-kenttä voi saada 4 eri arvoa, 1(*more*), 2(*start*), 4(*stop*) ja 8(*watchdog*). Muut kentät on esitelty jo aiemmin valtuutus-osiossa. Kirjanpito-osioon on lisätty kuitenkin tärkeitä attribuuttiarvopareja kuten *Task*_id, joka on tapahtuman tunnistekenttä. Näiden lisäksi on myös tärkeitä attribuuttiarvopareja liittyen aikaan kuten aloitus- ja lopetusajankohdat sekä aikavyöhyke. Tunnistekentän on pysyttävä samana aloitus ja lopetustapahtumissa, kuten kuviossa 37 on osoitettu (Carrel & Grant 2013, 34).



KUVIO 37. Aloitus/Lopetus task_id

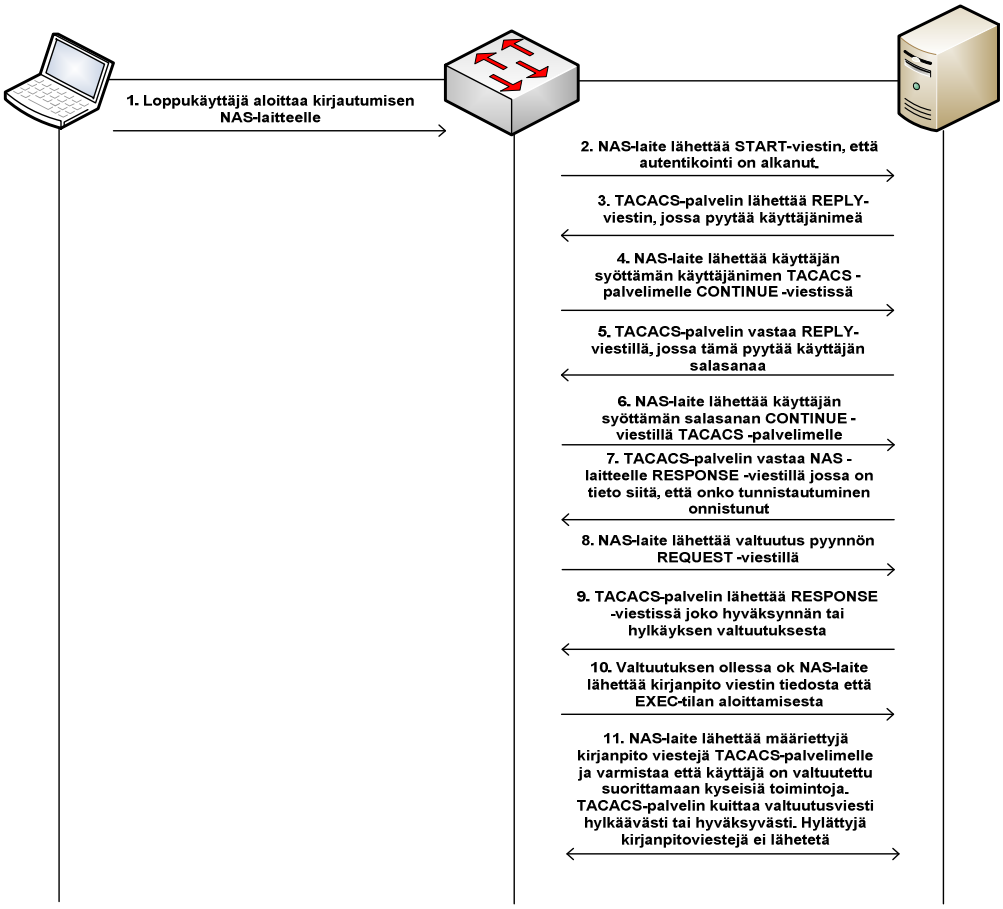
Seuraavana vuorossa on kirjanpidon vastausviestit. Vastausviestien tarkoituksena on ilmaista, että onko kirjanpito onnistunut. Tämä tarjoaa NAS-laitteelle parhaan mahdollisen tavan kertoa, että kirjaukset on suoritettu (Carrel & Grant 2013, 36). Seuraavassa kuviossa 38 on kirjanpidon vastausviesti.



KUVIO 38. TACACS+-kirjanpitovastausviesti

Status-kentän tehtävänä on kertoa NAS-laitteelle nimensä mukaisesti kirjanpidon tilasta, menikö viesti perille ja kuitattiinko se onnistuneesti vai tehdäänkö muita toimenpiteitä (Carrel & Grant2013, 37).

TACACS+ -protokollan AAA-tapahtumat on kuvattu järjestyksessä kuviossa 39.



KUVIO 39. NAS – TACACS-kommunikointi

3.4 Yhteenveto

Suurimmat eroavaisuudet TACACS+ ja RADIUS -protokollien välillä ovat siirtoyhteys-protokolla, pakettien salaus-mekanismit ja se, että TACACS+ muodostaa jokaisesta AAA osa-alueesta oman istunnon. Näistä seikoista johtuen TACACS+ soveltuu paremmin laitteiden keskitettyyn käyttäjähallintaan aktiivilaitteille ja RADIUS soveltuu paremmin käytettäväksi käyttäjien pääsynhallintaan verkkoliikennöinnin osalta. Taulukossa 6 on esitelty tiivistetysti eroavaisuudet.

TAULUKKO 6. TACACS+ vs. RADIUS

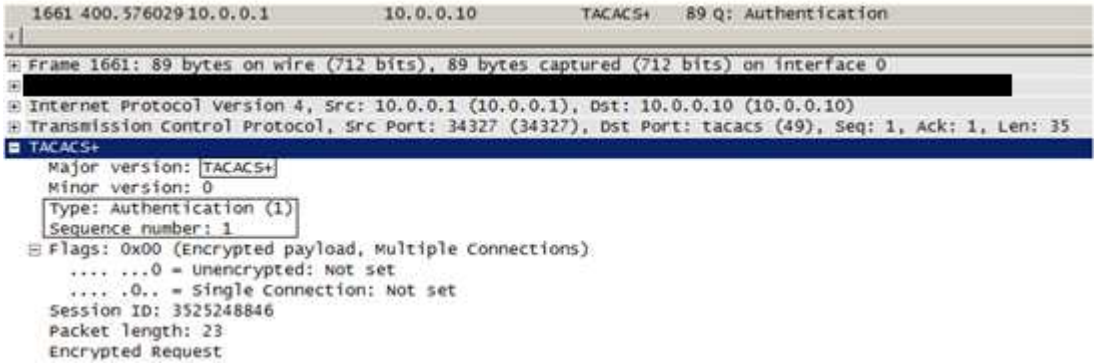
	TACACS+	RADIUS
Siirtoyhteysprotokolla	TCP	UDP
Portti	49	1812 ja 1813 (accounting)
Salaus	Kokopaketti	Vain salasana
Soveltuva käyttökohde	Laitteiden hallinta	Loppukäyttäjien pääsyn hallinta

Kuviossa 40 ja 41 on vertailtu Wireshark kuvakaappauksia RADIUS ja TACACS+-protokollien välillä. Kuvioista käy hyvin ilmi, että TACACS+ on huomattavasti suljetumpi ja näin ollen ilman jaettua salaisuutta paketeista saadaan hyvin vähän tietoa.

Kuviota 40 tarkastellessa voidaan huomata, että RADIUS-paketista saadaan selville ensimmäisenä, että minkälainen viesti on kyseessä (*Access-Request*). Seuraavana nähdään attribuutit joista suurin osa näkyy selkokielisenä. Paketista voidaan saada selville mm. Käyttäjätunnuksia, NAS-laitteen IP-osoitteita sekä *Calling-station-Id*, joka on tietoverkkoympäristössä loppukäyttäjän päätelaitteen IP-osoite.

KUVIO 40. RADIUS-autentikaatiopaketti

Kuviota 41 tarkastellessa huomataan, että TACACS+-paketista saadaan selville ainoastaan se, että protokollan ensisijainen versio on TACACS+. Pakettia tarkastellessa huomataan myös, että kyseessä on autentikaatio-paketti eli otsakkeessa olevat osiot. Kyseinen paketti on lähetetty loppukäyttäjältä palvelimelle päin, koska paketin sekvenssi numero on pariton.



KUVIO 41. TACACS+-autentikaatiopaketti

4 VAHTI

4.1 Yleistä

Valtionhallinnon tietoturvallisuuden johtoryhmä (VAHTI) on valtionvarainministeriön asettama hallinnon tietoturvallisuuden yhteistyön, ohjauksen ja kehittämisen elin. VAHTI:n tehtävänä on käsitellä tietoturvallisuutta koskevat säädökset, ohjeet, suositukset, tavoitteet, sekä muut tietoturvallisuuden linjaukset ja ohjata valtionhallinnon tietoturvatoimenpiteitä. VAHTI edistää toimintatavan kehittämistä julkishallinnon tietoturvatyössä. Tavoitteena on tietoturvallisuutta kehittämällä parantaa toimintojen luotettavuutta, jatkuvuutta, laatua, riskienhallintaa, varautumista ja edistää tietoturvallisuuden saattamista osaksi hallinnontoimintaa, johtamista ja tulosohjausta (Valtiohallinnon tietoturvallisuus 2013).

Sisäverkko-ohjeen tavoite on yleistää ja tehostaa menettelyitä sisäverkkojen rakentamisessa sekä tukea sopivan tietoturvatason käyttöönottoa organisaatiossa. Ohjeessa käsitellään kaikki merkittävimmät valtionhallinnon tietoturvallisuuden linjaukset ja tietoturvaan liittyvien toimenpiteiden ohjausasiat (Tietoturvallisuus 2013).

Opinnäytetyön toimeksiantajan vaatimus oli, että lähiverkkoon joka on suunniteltu laboratorioympäristöön, toteutettaisiin opinnäytetyössä VAHTI sisäverkko-ohjeen mukaisesti hallintayhteydet. Vaatimuksena oli, että toteutukseen tulee huomioida korotetun tason suositukset sisäverkon hallintaa silmällä pitäen.

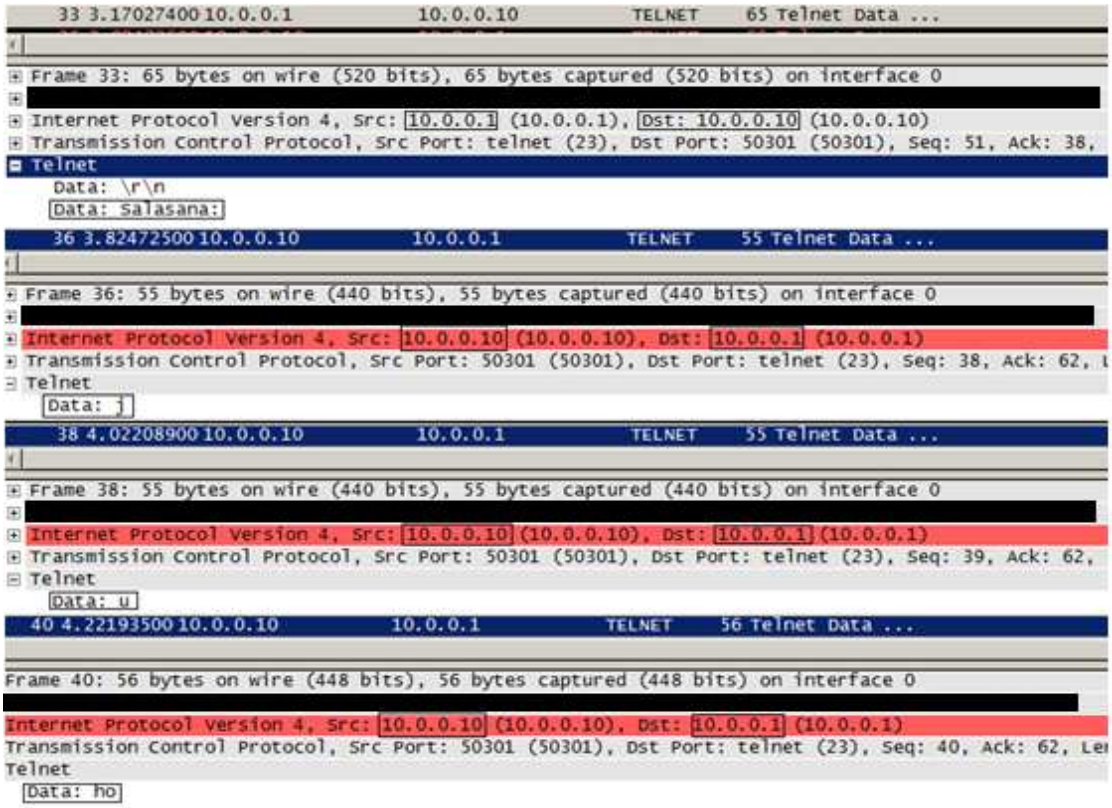
Työssä pyrittiin ottamaan jokainen VAHTI sisäverkko-ohjeen osa-alue huomioon, johon oli mahdollista vaikuttaa laboratorioympäristössä. Suurimmat työtä teettävät asiat olivat telnet:stä siirtyminen SSH-protokollaan ja käyttäjien keskittäminen yhteiseen tietokantaan, jotta geneerisestä käyttäjätunnuksesta päästään eroon sekä varmuuskopiointiin liittyvät viitteet.

4.2 Telnet & SSH

Työn kannalta käyttäjähallinnan lisäksi oleellinen asia oli VAHTI-ohjeen luku 16 eli ”Verkon hallinta/valvonta”. Kyseisessä luvussa käydään läpi kuinka tietoturvallinen hallinta/valvonta ympäristö tulisi toteuttaa.

Ensimmäisenä työssä tuli korvata laitteiden suojaamaton hallintayhteys (telnet) salatulla SSH-yhteydellä. Telnet-yhteys ei suojaa millään tasolla liikennettä, ei edes salasanoja. Koska hallintalinjoihin asetetaan SSH-yhteys, pyritään varmuuskopiointi suorittamaan käyttämällä SCP:tä (secure copy), sillä se on huomattavasti tietoturvallisempi kuin ftp tai tftp. SSH-yhteyttä käyttäen ei ulkopuolinen pääse tunnistamaan liikenteestä mitä muutoksia verkkoon suoritetaan, joten olisi erikoista käyttää koko konfiguraatiotiedostojen siirtämiseen tietoturvattomampaa tftp-protokollaa.

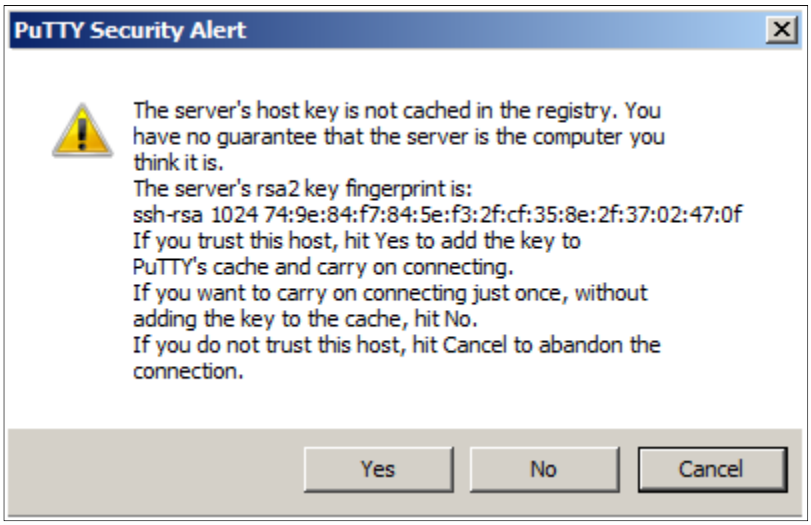
Kuviosta 42 on esitetty miten tietoturvaton telnet-yhteys on. Mikäli kaappaaja pääsisi salakuuntelemaan kirjautumistapahtumaa, hän saisi heti selville käyttäjätunnukset ja salasanat. Kuviossa 42 on esitetty kirjautumistapahtuma verkkolaitteen osoitteeseen 10.0.0.1 osoitteesta 10.0.0.10. Ensiksi verkkolaite lähettää viestin ’Salasana:’, johon sitten käyttäjä on vastannut kolmessa osassa merkkijonon: ”juho”.



KUVIO 42. Telnet salasana

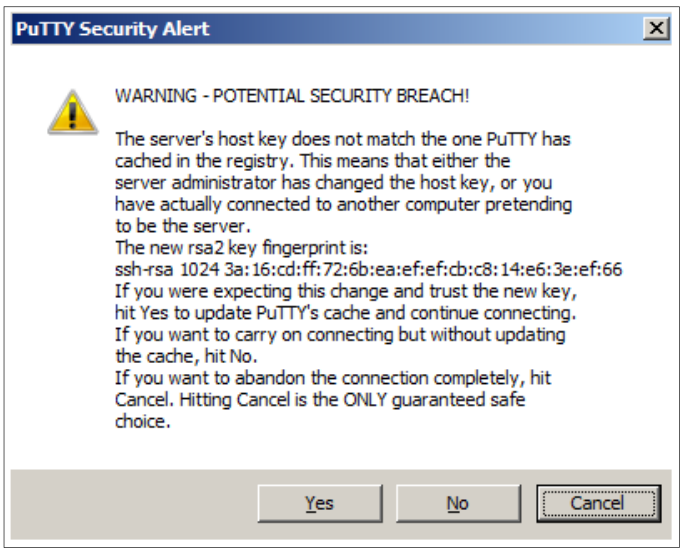
SSH eli secure shell on nykypäivänä yhteys, jolla tulisi korvata tietoturvaton telnet-yhteys. SSH:sta on kehitetty kaksi versiota 1 ja 2. Versio 1 sisältää useita tietoturva ongelmia liittyen kryptografiaan, jotka on korjattu SSH:n uudemmassa versiossa 2 (Dwivedi Chapter 1 2013).

SSH-istunto käynnistyy kun asiakas yrittää avata TCP-yhteyden oletusarvoisesti porttiin 22, tässä tapauksessa reitittimeen jonka on kuunneltava kyseistä TCP-porttia. Kun TCP-yhteys on avattu, lähettää reititin oman julkisen avaimensa asiakkaalle. Kuviossa 43 on esitetty tapahtuma jossa on otettu PuTTy-pääteohjelmalla SSH-yhteys reitittimeen ja reititin lähettää avaimensa sormenjäljen, joka pitää hyväksyä jotta SSH-yhteys syntyisi. Toisin sanoen tällä pyritään takamaan se, että laite on se joksi sitä luulet. Kyseistä ilmoitusta ei tule, mikäli et ole ottamassa laitteeseen ensimmäistä kertaa yhteyttä ja avain on asennettu päätteen välimuistiin.



KUVIO 43. SSH yhteyden avain

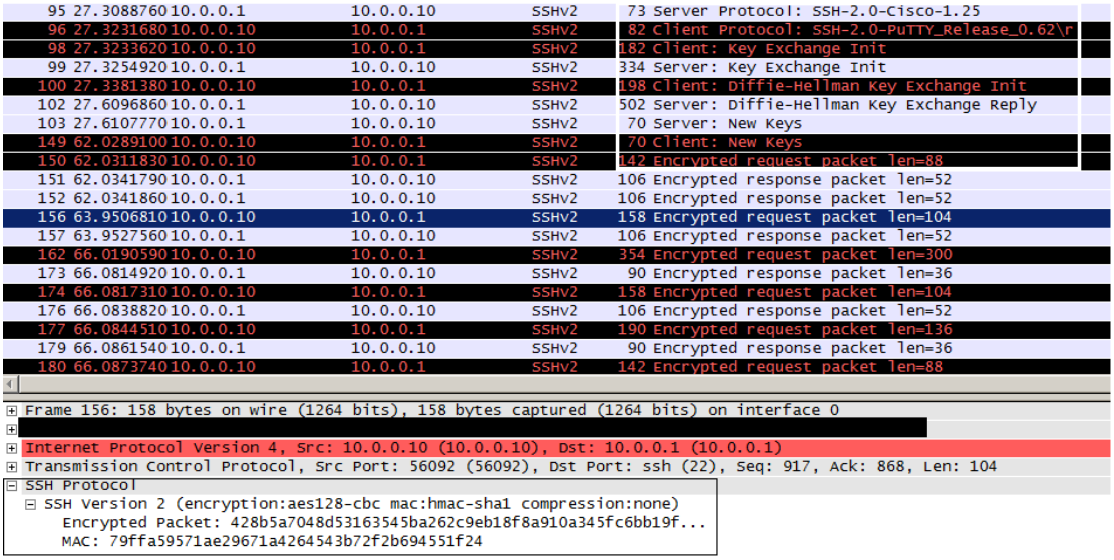
Asiakaslaitteet pitävät tietokantaa tunnetuista palvelimista ja niiden avaimista. On olemassa kuitenkin tapauksia, joissa avain saatetaan vaihtaa uuteen johon onneksi pääteohjelmat pääasiassa reagoivat. Kuviossa 44 on esitetty varoitusviesti kun reitittimen lähettämä avain ei vastaa avainta, jonka PuTTy-pääteohjelma on tallentanut. Tällaisissa tapauksissa on kuitenkin hyvä varmistaa verkon ylläpidolta, että avainta on varmasti vaihdettu jotta vältytään ikäviltä tietoturva vahingoilta. Vastaavasti voidaan ylläpitää tietokantaa, jossa on kaikki julkisten avaimien sormenjäljet joihin sitten työntekijät voivat verrata pääteohjelman tarjoamaa sormenjälkeä.



KUVIO 44. SSH yhteyden avain on vaihtunut

Edellä olevissa tapahtumissa reititin ja asiakasohjelma ovat nyt tunnistaneet toisensa. Käyttäjän tunnistamiseen voidaan käyttää erilaisia menetelmiä kuten julkiseen avaimeen perustuva kirjautuminen tai käyttäjätunnus-salasana-parin menetelmää (Miten SSH toimii 2013).

Kuviossa 45 on osoitettu kuinka SSH-yhteys eroaa telnet-yhteydestä. Ensimmäisenä kuviossa tapahtuu avaimen vaihto, jonka jälkeen SSH-yhteys muodostuu. SSH-paketteja tarkastellessa Wireshark-ohjelmalla ei paketeista saada kaivettua paljoa tietoa ilman korkeaa ammattitaitoa. Kuvio 45 on otettu tapahtumasta, jossa avaimet ovat vaihdettu palvelimella. Avaimien vaihtoon reititin ja asiakas on käyttänyt Diffie-Hellman avaimenvaihtoprotokollaa. Kuviota 45 tarkastellessa saamme selville, että kyseessä on SSH:n versio 2, salaukseen on käytetty 128-bittistä AES salausta ja eheysalgoritmina on käytetty hmac-sha1:stä.



KUVIO 45. SSH-dataa

4.3 VAHTI sisäverkko-ohjeen tarkistuslistat

Valtionvarainministeriön luoma ohje sisäverkolle on julkinen vuodelta 2010. Ohjeessa oli paljon asioita joihin näin pienellä verkon osa-alueella pystyi vaikuttamaan. Opinnäytteessä ei oteta kantaa siihen, että onko kaikki kyseiset seikat jo konfiguroitu toimeksiantajan verkkoon vai ei.

Liitteeseen 8 on listattu osa-alueet, joihin työssä pystyttiin vaikuttamaan. Sisäverkko-ohjeessa oli osa-alueita kolmesta eri tarkistuslistasta, jotka työssä oli mahdollisuus ottaa huomioon laboratorioympäristöä silmällä pitäen.

- Tunnistautumisen tarkistuslista (15)
- Hallinnan/valvonnan tarkistuslista (16)
- Jatkuvuussuunnittelun tarkistuslista (17)

Opinnäytetyön toteutuksen jälkeen tehdään yhteenveto siitä, että pystyttiinkö jokainen listattu asia toteuttamaan (VAHTI tiivistelmä 2013).

5 TUOTTEEN VALINTA KESKITETTYYNKÄYTTÄJÄHALLINTAAN

5.1 Tuotteiden karttoittaminen

Tuotetta keskitettyyn käyttäjähallintaan miettiessä ja niitä kartoittaessa, tuotteiden määrä kasvoi jatkuvasti. Joka kerta tuotteita kartoittaessa uudelleen, löytyi jokin uusi tuote, joka sisälsi RADIUS-protokollan, TACACS+-protokollan tai molemmat. Tuotteet tuli siis rajattiin siis mahdollisimman nopeasti. RADIUS-palvelinta on tarjolla lukuisia määriä ilmaisia tuotteita. TACACS+-palvelinta ei löytynyt (Trial-versioita lukuun ottamatta) ilmaisia kokonaisuuksia, joiden uskottiin toimivan stabiilisti. Näistä syistä RADIUS-palvelimeksi vertailuun valittiin FreeRADIUS, sillä se oli entuudestaan tuttu ja siihen olisi mahdollista luoda graafinen käyttöliittymä käyttäjien, NAS-laitteiden, attribuuttien sekä muiden tarvittavien tietojen lisäämiseksi. TACACS+-palvelinta miettiessä tuli kartoittaa monia tuotteita, sillä kyseessä oli varmasti kaupallinen tuote. Haku netistä tapahtuikin lähiverkon hallintaan tarkoitetuilla hakusanoilla ja tuotteiden kirjo oli valtava. Otin vertailuun itselleni taulukossa 7 esitetyt tuotteet.

Aluksi tuntui, että vertailussa oli tuotteita liikaa. Tuotteita hieman enemmän tutkiessa, alkoi tuotevalikoima suppememaan melko nopeasti. Cisco ISE-tuotteen nykyinen versio (1.1) ei tukenut TACACS+:aa mutta versioon 2.0 on ilmeisesti tulossa myös TACACS+-toiminne, jonka jälkeen tämä voisi olla varteen otettava vaihtoehto. Cisco Prime paljastuikin ainoastaan lähiverkon hallintatyökaluksi, ei siis niinkään käyttäjien hallintaan. Nämä kaksi tuotetta karsiutui hyvin nopeasti pois valikoimista. Cisco ACS for Windows v. 4.2 sisälsi TACACS+:an, mutta sekin jouduttiin karsimaan melko nopeasti pois valikoimista, sillä uusin Windows-versio, jota kyseinen ohjelmisto tuki oli 32-bittinen Windows 2003 SP1. Cisco ACS-tuoteperheestä löytyi myös appliance-versio, eli räkkiin asennettava fyysinen palvelinrauta.

TAULUKKO 7. Tuotteet

Tuote	RADIUS	TACACS+
CISCO Identity Services Engine (ISE)	x	
CISCO Access Control Server (ACS)	x	x
Hewlett Packard Intelligent Management Center (IMC)	x	x
FREE radius	x	
CISCO Prime		
Cisco ACS appliance	x	x

Toimeksiantajalle syntyi nopeasti mielipide, että TACACS+ on ehdoton protokollavalinta. VAHTI-ohjeessa on jo perustasolla suosituksena, että on pystyttävä seuraamaan mitä on tehty, kuka on tehnyt ja milloin on tehty eli niin sanottu ”*Audit trail*” on onnistuttava. RADIUS ei pysty suoriutumaan komentojen kirjauksesta ulkoiselle palvelimelle.

Tuotteista laboratorio kartoitukseen valittiin Hewlett Packardin tuote Intelligent Management Center ja Cisco ACS appliance-versio. Tuotteista kumpikaan ei ollut entuudestaan tuttu ja näin ollen joudutiin hieman enemmän tutustumaan molempiin tuotteisiin.

5.2 Cisco Secure Access Control Server

Cisco ACS-palvelin on suunniteltu täysin AAA-tuotteeksi. Palvelinta voidaan hyödyntää niin laitteiden lokitietojen keräämiseen, pääsynhallinnan rajoittamiseen verkkoon (802.1x + RADIUS) tai pääsynhallinnan rajoittaminen laitteille. (TACACS+)

Laite on myös mahdollista klusteroida jolla mahdollistetaan korkea saatavuus. Laboratorioympäristössä käytössä oli ainoastaan yksi laite, joten vikasietoisuuden kannalta laboratorioympäristö ei ollut paras mahdollinen. ACS-palvelimelle ei löydetty tietoa siitä, että kuinka monelle NAS-laitteelle sillä on tuki. Cisco ACS-palvelimelle määritetään esiasennus vaiheessa alkuparametrit komentoriviltä käsin, mutta tämän jälkeen laitetta käytetään pääasiassa graafisen käyttöliittymän kautta. ACS-palvelimella ei ole valmistajakohtaisia rajoitteita, sillä NAS-laitteena voi toimia mikä tahansa laite,

joka tukee TACACS+ tai RADIUS-protokollaa. Ciscon tuotteessa ei ollut tarvetta mietiä laitevaatimuksia, sillä kyseessä oli kiinteä räkkiin asennettava tuote.

5.3 Hewlett packard intelligent management center

HP:n tuote (IMC) on suunniteltu kokonaisvaltaiseen verkon hallintaan sekä monitorointiin. IMC käyttää hyväkseen modulaarista arkkitehtuuria, eli siihen voidaan liittää uusia moduuleita tarpeen tullen, kuten *VPN-manager*, *User Access Manager* tai *TACACSs+ Authentication Manager*. IMC:ssä voidaan myös hallitusti konfiguroida laitteita, kuten asettamalla niille VLAN:eja tai pääsylistoja. IMC tukee myös kolmannen osapuolen laitteita, joka tekee IMC:stä melko joustavan käyttää erilaisissa monitoimittajaympäristöissä. IMC-palvelin on myös asennettavissa Windows ja Linux alustoille sekä tuotteesta on saatavilla Standard ja Enterprise-versiot. Laitevaatimukset IMC-palvelimelle vaihteli sen mukaan, mitä laitteelta odotettiin. Seuraavat minimilaitevaatimukset riittivät opinnäytteessä käytettävään ratkaisuun (Hewlett Packard 2013):

- Intel® Pentium® 4 3.0 GHz Prosessori
- 4 GB RAM muistia
- 50 GB kovalevy tilaa
- min. 10 MB verkkokortti
- Windows® server 2008 r2 SP1

5.4 Valinta

Molemmat tuotteet asennettiin ja testattiin laboratoriossa. HP:n IMC asennettiin Windows 2008 r2 Enterprise-palvelimelle. Cisco ACS:stä oli käytössä räkkiin asennettava palvelin. HP IMC oli kattava kokonaisuus, kun taas Ciscon ACS on pääasiassa pääsynhallintaa varten oleva kokonaisuus. IMC vaati asennuksen yhteydessä, että käytetään ulkoista tietokantaa johon tiedot varastoidaan. Tästä syystä 2008 r2-palvelimelle tuli asentaa Microsoft SQL Server 2008 r2 tietokantapalvelinohjelmisto.

IMC:stä on saatavilla Standard ja Enterprise-versiot. Standard-versio oli riittävä opinnäytetyöhön, mutta TACACS+ ei sisältynyt siihen, joten se tuli asentaa erillisenä moduulina. IMC tarjosi erilaisia ominaisuuksia verrattuna ACS-palvelimeen, kuten automatisoitu laitteiden konfiguraatioiden varmuuskopiointi ja VLAN-hallinta. Hinta ero oli kuitenkin niin suuri kyseisten tuotteiden välillä joten parhaaksi nähtiin se, että perehdytään edullisempaan tuotteeseen joka oli ACS. Työssä pyrittiin toteuttamaan VAHTI-ohjeen mukaiset toiminnot kuten varmuuskopiointi, jollain muulla tavalla. Laboratorioympäristössä oli käytössä Linux-palvelimia joihin on mahdollista ohjelmoida pieniä skriptejä, joilla voidaan suorittaa esimerkiksi varmuuskopiointi.

Cisco ACS valittiin käyttöön mm. edullisemman hinnan puolesta sekä siinä ei ollut niin paljon ylimääräisiä ominaisuuksia, joten näin ollen opinnäytetyön kannalta turhista ominaisuuksista ei tarvinnut maksaa. Toimeksiantajalla on myös oma valvontaa suorittava yksikkönsä jonka takia HP:n tuotteen muut lisäominaisuudet eivät olleet hyödyllisiä, sillä yksiköllä on käytössä jo kilpailutettu verkonvalvonta työkalunsa. Tietoverkon kanssa työskentelevät henkilöt toki voivat valvoa itselleen tärkeitä kohtia verkossa, mutta näihin tarkoituksiin IMC-tuote olisi ollut ylimitoitettu. Vaikka laboratoriossa tutkittiin molempia tuotteita melko syvällisesti, niin työssä ei dokumentoida palvelimista kuin ACS:n asennus ja konfigurointi.

6 TOTEUTUS

6.1 Yleistä

Toteutus osio alkoi tutustumisella valittaviin palvelimiin ja niiden ominaisuuksiin. Kun valinta oli suoritettu, ryhdyttiin tutkimaan valittuja palvelimia syvemmin ja samanaikaisesti aktiivilaitteiden konfiguraatioita. Seuraava askel oli laboratorioympäristön suunnittelu IP-osoitteineen ja topologioineen. Laboratorioympäristössä käytössä ei ollut rajattomat resurssit, joten näin ollen työssä ei ole panostettu korkeaan saatavuuteen, silmukanestoihin, porttikanaviin, kytkinpinoihin tai muihin perinteisiin lähiverkon tekniikoihin.

Laboratorioon suunniteltiin kuvion 46 mukainen ympäristö, joka mahdollisti testauksen ja todentamisen TACACS+-protokollan ja AAA-arkkitehtuurin eri osa-alueilla. Ympäristössä käytettiin *'Router on the stick'*-reititystä siitä syystä, että *sw1* ja *r1*-laitteiden välillä käytettiin hubia johon oli kytketty monitorointi työasema, joka mahdollisti jatkuvan liikenteen tutkimisen *VLAN*:ien välillä. Ympäristössä käytettiin taulukon 8 osoittamia laitteita. Taulukossa ei ole esitelty ohjelmistoversioita eikä tarkentavia malleja laitteista.

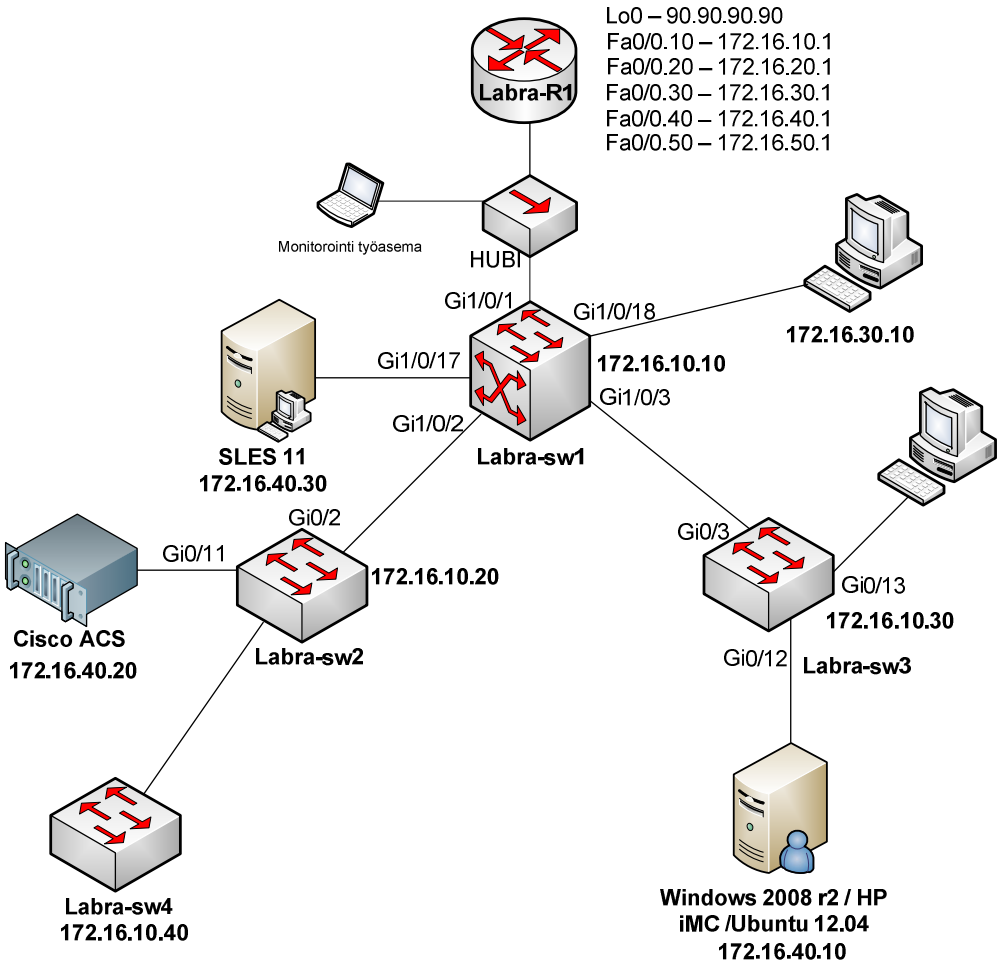
TAULUKKO 8. Laboratoriolaitteet

Laite	Tieto
Labra-r1	Cisco 1841
Labra-sw1	Cisco 3750
SLES	Suse Linux Enterprise Server
Cisco ACS	Cisco secure Access Control Server 1180
Labra-sw2	Cisco 2960
Labra-sw3	Cisco 2960
Labra-sw4	Dell PowerConnet 6224
Windows 2008 r2	Virtual Box(win7) dual boot Ubuntu 12.04

Laboratorioon suunniteltiin taulukon 9 mukainen IP-osoitteistus sekä VLAN-suunnitelma.

TAULUKKO 9. VLANit ja IP-osoitteet

VLAN	Verkko	Käytettävät osoitteet	Verkkomaski	nimi
10	172.16.10.0	172.16.10.1 - 254	m24	Hallinta
20	172.16.20.0	172.16.20.1 - 254	m24	Palvelimet
30	172.16.30.0	172.16.30.1 - 254	m24	Adminit
40	172.16.40.0	172.16.40.1 - 254	m24	Tuotanto
50	172.16.50.0	172.16.50.1 - 254	m24	Vieras

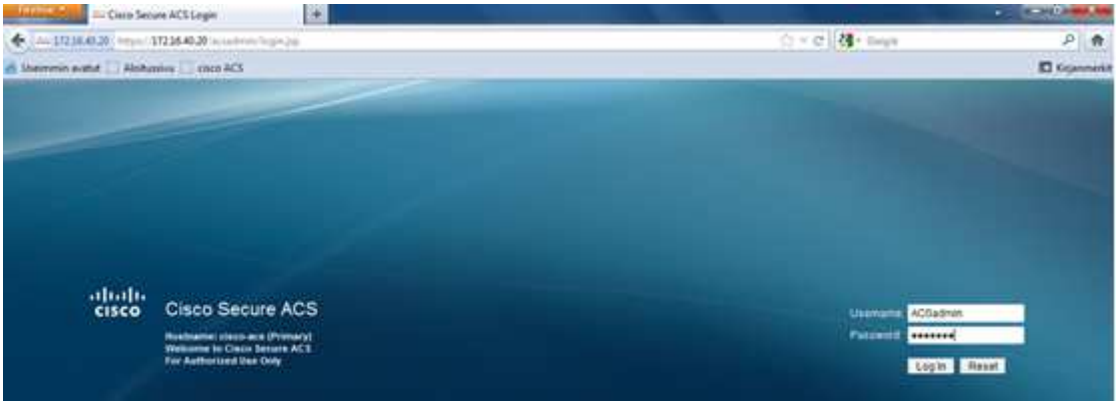


KUVIO 46. Laboratorioympäristö

Vaikka laboratorioympäristöön oli asennettu HP iMC-palvelin joka ei tullut käyttöön, pystyttiin alustana olevaa Windows 2008 r2-palvelinta hyödyntämään mm. Windows aktiivihakemistona (Active Directory). Aktiivihakemistoa käytetään työssä ACS-palvelimen ulkoisena käyttäjätietokantana.

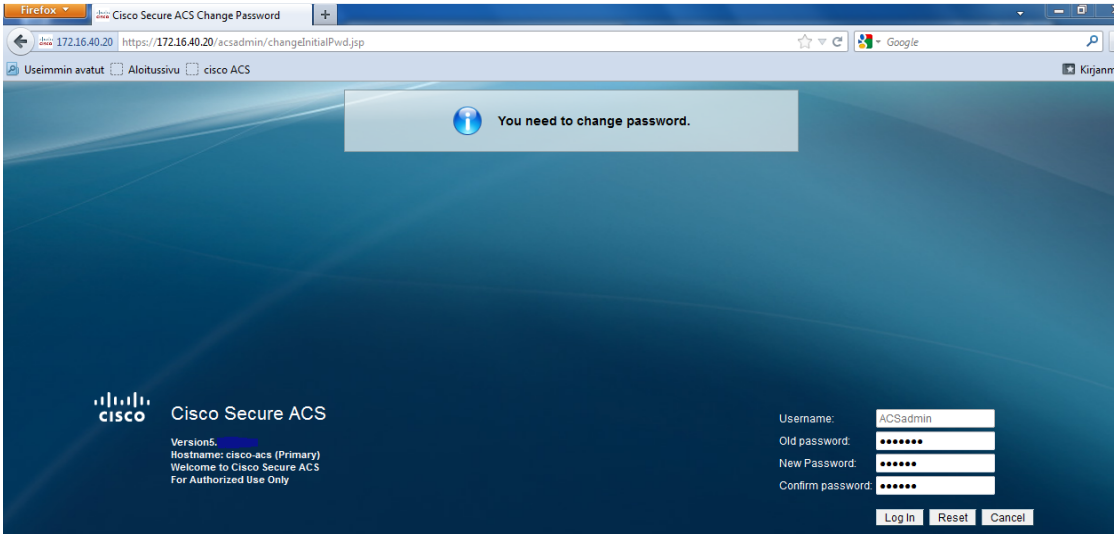
6.2 Cisco ACS

ACS-palvelimen pystyttäminen alkoi sillä, että siihen asennettiin uusi ohjelmistoversio. Liitteessä 2 on esitelty ja selitetty palvelimen esiasennuksen eri vaiheet. Palvelimen peruskonfiguraatioiden jälkeen palvelinta hallitaan pääasiassa verkkoselaimen kautta käyttäen HTTPS-protokollaa. Kuviossa 47 on esitelty kirjautumisikkuna, kun laitteelle kirjaudutaan ensimmäistä kertaa.



KUVIO 47. Ensimmäinen kirjautuminen ACS www-sivustolla

Ensimmäisellä kerralla laitteelle pitää kirjautua ACSadmin-tunnuksella. Samalla kerralla tulee vaihtaa ACSadmin-käyttäjän salasana uuteen ACS-palvelimen pyynnöstä. Kuviossa 48 on esitelty tapahtuma.



KUVIO 48. Salasanan vaihto ensimmäisellä kirjautumiskerralla

Käyttäjän kirjauduttua laitteelle ensimmäistä kertaa, tulee palvelinohjelmisto lisensoida. Tämän jälkeen ACS-palvelin on käyttövalmis.

Liitteessä 3 on toimeksiantajalle luotu ohje ACS-palvelimen konfiguroinnista, kuten käyttäjäryhmien, käyttäjätunnuksien ja profiilien luomisesta. Toimeksiantajan verkossa on suuri määrä laitteita, josta syystä samaisessa liitteessä on esitelty miten ACS-palvelimelle voidaan viedä yhdellä tiedostolla useita aktiivilaitteita. Liitteessä 4 on esitetty kuinka suoritetaan ACS ja AD-palvelimien integroiminen.

6.3 Aktiivilaitteiden konfiguraatiot

Yleisesti konfigurointi lähti liikkeelle sillä, että tutustuin kunkin laitevalmistajan kyseisen tuotteen *”Config Guide”*-manuaaliin. Opinnäytteen aktiivilaitteiden perusasetukset menivät selkärangasta laitteisiin mutta AAA-komennot, aika-komennot ja VAHTI-ohjeen eri osa-alueet eivät olleet entuudestaan tuttuja.

6.3.1 Cisco konfiguraatiot

Kun TACACS+-palvelin saatiin asennettua, oli aika ryhtyä konfiguroimaan aktiivilaitteita. Ensimmäisenä suunniteltiin Ciscon konfiguraatiot, sillä kyseisiä laitteita oli laboratoriossa eniten ja kyseinen CLI oli entuudestaan tuttu. Tämä helpotti konfiguroinnin aloittamista suuresti.

Laitteisiin syötettiin ensimmäisenä komento, joka ottaa käyttöön AAA-arkkitehtuurin ja aktivoi *default*-linjat *vty* ja *console*-yhteyksille:

#aaa new-model

AAA-arkkitehtuurin konfigurointia aloittaessa, oli loogisinta aloittaa konfigurointi ensimmäisestä A:sta, eli *Authentication*-osuudesta.

Ensimmäisenä määritettiin oletus autentikaatiometodiksi TACACS+ komennolla:

#aaa authentication login default group tacacs+

Seuraavaksi tuli luoda sääntö, jonka avulla laitteisiin on mahdollista kirjautua konsolilinjan kautta käyttäen paikallista tunnusta vaikka TACACS+-palvelin ei olisi saatavilla:

#aaa authentication login CONSOLE local

Edellä luotiin autentikaatiometodi nimeltä *CONSOLE*, mikä tulee liittää konsolilinjaan komennoilla:

#line con 0

#login authentication CONSOLE

Jotta sääntö *CONSOLE* olisi käytännöllinen, tulee laitteelle luoda hätävara tunnus ja salata salasanat:

#username vaikeasTiArvAttAva password ToDeLlAVaikEa

#service password-encryption

Toisena A:na AAA-arkkitehtuurissa tulee *Authorization* eli valtuutus. Valtuutuksessa haluttiin, että käyttäjä pääsee suoraan *exec*-tilaan, mikäli tämä on autentikoitunut:

#aaa authorization exec default group tacacs+ if-authenticated

Konsolin kautta kirjautuessa ei laitteelle tarvitse antaa erikseen valtuutus komentoa. Seuraavana valtuutukseen komennettiin komentojen valtuuttaminen:

#aaa authorization config-commands

Viimeisenä AAA-arkkitehtuurin osana on *Accounting* eli kirjanpito. Kyseistä osiota konfiguroitaessa on hyvä pohtia, että mitä asioita halutaan laitteilta kirjata ylös. Kirjautumiset jäävät ACS-palvelimen lokille automaattisesti, joten näitä ei tarvitse erikseen lokittaa. VAHTI-ohjetta silmällä pitäen on tärkeää, että konfiguraatiomuutokset lokitetaan ja mikäli laitteelle annetaan esimerkiksi uudelleenkäynnistämiseen johtava komento, kirjataan se myös palvelimelle. Konfiguraatiokomentoja lokittaessa voidaan komennot rajata *privilege 15*-tilaan, sillä alemmat privilege tilat eivät voi oletuksena suorittaa konfiguraatioita:

#aaa accounting commands 15 default start-stop group tacacs+

Laitteen järjestelmälliset kirjaukset kuten uudelleenkäynnistys tapahtuu komennolla:

#aaa accounting system default start-stop group tacacs+

Laitteelle on konfiguroitu nyt toiminteet käyttämään TACACS+-palvelinta, joten seuraavaksi on määriteltävä TACACS+-palvelin:

#tacacs-server host 172.16.40.20 key labra

Kuten liitteessä 3 on esitetty, labra-r1-laitteen NAS IP-osoitteeksi määritettiin 172.16.10.1 eli alirajapinnan *'fastethernet0/0.10'* IP-osoite. Tästä syystä reitittimelle tulee vielä syöttää komento:

#ip tacacs source interface fastethernet0/0.10

Nyt laite käyttää palvelimen kanssa kommunikointiin oikeaa IP-osoitetta. Mikäli kytkimillä tai muilla aktiivilaitteilla on useampia IP-osoitteita, tulee niille komentaa lähde-rajapinta TACACS+-kommunikointia varten. Kytkimille opinnäytetyössä luotiin

ainoastaan yksi SVI-rajapinta (Switch Virtual Interface, interface vlan), jolle annettiin IP-osoite ja tästä syystä lähderajapinta-komentoa ei tarvitse asettaa kytkimille.

AAA-konfiguraatioiden jälkeen voidaan suojaamaton telnet vaihtaa turvallisempaan SSH-protokollaan. SSH-toiminto tarvitsee avaimien luomiseen isäntänimen sekä toimialueen nimen. Kyseiset toiminnot suoritettiin komennoilla:

#hostname Labra-r1

#ip domain-name labra.local

Kun nämä määritykset on suoritettu, voidaan laitteella generoida avainparit, joita käytetään SSH:n yhteydessä:

#crypto key generate rsa

1024

y

Edellä luotiin 1024-bittinen avain. Pakotetaan käyttöön vielä SSH versio 2, mikä on turvallisempi kuin versio 1:

#ip ssh version 2

Laitteille on hyvä vielä komentaa käyttöön vain SSH, jotta käyttäjät pakotetaan käyttämään turvallista SSH:ta ja telnetin käyttö on estetty:

#line vty 0 4

#transport input ssh

Cisco Systemsin laitteisiin pitää vielä komentaa SCP-palvelu päälle erikseen komennolla:

#ip scp server enable

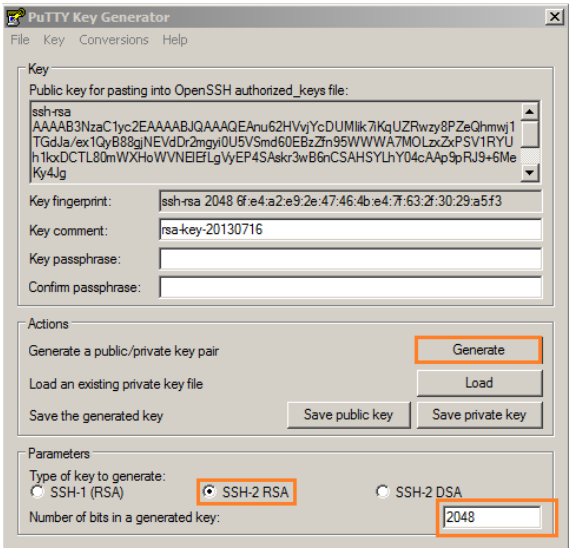
Laitteille määriteltiin kelloasetukset, sillä jokaisen verkon aktiivilaitteen on syytä olla oikeassa ajassa tai ainakin synkronoitu muiden sisäverkon laitteiden kanssa samaan aikaan.

Kelloasetukset konfiguroitiin seuraavalla tavalla:

#clock timezone EET 2

#ntp server 172.16.40.10

VAHTI sisäverkko-ohjeessa on kohta jossa määritellään, että pelkkä käyttäjätunnussalasana pari ei riitä. Laboratorioympäristöön sain käyttööni Cisco Systemsin uuden IOS-version 15.02. Kyseinen ohjelmistoversio mahdollistaa avaimeen perustuvan tunnistautumisen. Kuviossa 49 luodaan PuTTy keygen-ohjelmalla (avain generaattori) avainpari, jota käyttäjä ja SSH-palvelin käyttävät. Avaimen voi kopioida esimerkiksi WWW-sivuille tai muistio-tiedostoon, josta se sitten kopioidaan laitteelle kuvion 50 mukaisesti.



KUVIO 49. PuTTy Keygen-ohjelmistolla avaimenluominen

Kuviossa 50 on havainnollistettu avaimen kopiointitapahtuma Labra-sw2-laitteelle.

```
Labra-sw2(conf-ssh-pubkey)#username juho
Labra-sw2(conf-ssh-pubkey-user)#ke
Labra-sw2(conf-ssh-pubkey-user)#key-s
Labra-sw2(conf-ssh-pubkey-user)#key-string
Labra-sw2(conf-ssh-pubkey-data)#
Labra-sw2(conf-ssh-pubkey-data)#$QAAAQEAxbDRquAKS8Gs4usc6EHYySz3lziBJXhTZDC8
Labra-sw2(conf-ssh-pubkey-data)#$ZB2lHx8QR/7SZFJPrbd14fkRBe4sZR2/GodEcQdnrNF
Labra-sw2(conf-ssh-pubkey-data)#$vT2A5xa5q8u4e4u9ymPcLqdlDexZetmoRTVT8LjoFUo
Labra-sw2(conf-ssh-pubkey-data)#$ltf5lcaMN4LInXPrT2hz1uFHXyg4N7pRaINc1iWTqFj
Labra-sw2(conf-ssh-pubkey-data)#$imYRPyAlmi6JTEnt+/RBR8J1ppfd1SZoQEPh0ewl2/F
Labra-sw2(conf-ssh-pubkey-data)#$NxnVZaPfcMP35+jalmPJPFQt6+u52FO2CTRQ/qw==
Labra-sw2(conf-ssh-pubkey-data)#exi
Labra-sw2(conf-ssh-pubkey-user)#exi
Labra-sw2(conf-ssh-pubkey)#exi
Labra-sw2(config)#
```

KUVIO 50. SSH-avaimen asettaminen aktiivilaitteelle

Aktiivilaitteelle ei tarvitse tehdä muita konfiguraatioita kuin asettaa avain halutulle käyttäjätunnukselle:

#ip ssh pubkey-chain

#username juho

#key-string

#<avain> (Copy + Paste)

#exit

#exit

#exit

Kyseinen toiminto näkyy laitteen konfiguraatioissa kuvion 51 osoittamalla tavalla.

```
 name Palvelimet
!
vlan 50
 name Vieras
!
ip ssh version 2
ip ssh pubkey-chain
  username juho
   key-hash ssh-rsa D824BBA64E2F88F133B3AA77845A4DEC
ip scp server enable
```

KUVIA 51. Konfiguraatiomuodossa avaimen tiiviste

Kuviossa 52 on esitelty, miltä näyttää verkkolaitteelle kirjautuminen käyttäen SSH-avainta.

```
Using username "juho".
Authenticating with public key "rsa-key-20130723"

Labra-sw2#
```

KUVIA 52. Kirjautuminen SSH-avaimella verkkolaitteelle

Lopuksi määritellään vielä pääsylistat, joilla pystyttiin rajaamaan hallintaa verkkolaitteille. Ciscon laitteille luotiin laajennettu pääsylista, jonka avulla luotiin pääsy SSH:lla osoitteista 172.16.40.10 ja 172.16.40.30 sekä 172.16.40.10 osoitteesta sallittiin SNMP-kyselyt, sillä kyseisellä raudalla pyöri *”dualboottina”* Windows 7 kanssa Ubuntu 12.04 lts. Lopuksi pääsylista tuli vielä liittää VTY-linjoihin, jotta sen merkitys tuli voimaan. Kyseinen toiminto luotiin komennoilla (Cisco Config Guide 2013):

#accesslist extended 101 permit tcp 172.16.40.10 host 172.16.10.1 eq 22 log

#accesslist extended 101 permit tcp 172.16.40.30 host 172.16.10.1 eq 22 log

#accesslist extended 101 permit udp 172.16.40.10 host 172.16.10.1 eq snmp log

#line vty 0 4

#access-class 101 in

6.3.2 Dell konfiguraatiot

Dell-laitteistojen konfiguraatiot eivät olleet entuudestaan juurikaan tuttuja mutta laitteita hieman tarkastelemalla sekä ”Dell PowerConnect PCM6220, PCM6348, PCM8024, PCM8024-k CLI Reference Guide”-manuaalia selaamalla kuitenkin saatiin oleelliset konfiguraatiot suunniteltua laitteille. Dellin laite joka oli laboratoriossa käytössä, oli sen verran vanha, ettei siitä voinut kerätä Accounting-osiossa määriteltyjä komentoja. Dellin laitteisiin konfiguroidaan ensimmäisenä AAA-arkkitehtuurin *Authentication*-osuus. Ensiksi luodaan sääntö jonka nimi on console, joka sallii kirjautumisen paikallisilla tunnuksilla, oletus kirjautumismetodiksi asetetaan TACACS+-autentikointi ja enable tilaan sallitaan pääsy ilman erillisiä toiminteita:

#aaa authentication login console local

#aaa authentication login enable console none

#aaa authentication login default tacacs

#aaa authentication login enable default none

Seuraavaksi määritellään TACACS+-palvelin:

#tacacs-server host 172.16.40.20

#tacacs-server key labra

Seuraavaksi konfiguroidaan SSH:n versio 2 päälle, luodaan avaimet sekä liitetään autentikaatiot oikeisiin linjoihin:

#ip domain-name labra.local

#crypto key generate rsa

1024

y

#ip ssh server

#ip ssh protocol 2

#line ssh

#login authentication default

#enable authentication default

#line console

#login authentication console

#enable authentication console

Laitteille määriteltiin kelloasetukset, sillä jokaisen verkon aktiivilaitteen on syytä olla oikeassa ajassa, tai ainakin synkronoitu muiden laitteiden kanssa samaan aikaan. Kelloasetukset konfiguroitiin seuraavalla tavalla:

#clock timezone 2 minutes 0 zone ”EET”

#sntp unicast client enable

#sntp server 172.16.40.10

Lopuksi vielä estetään telnetin käyttö luomalla hallintapääsylista (management access list) (Dell Config Guide 2013):

#management access-list Hallinta

#permit ip-source 172.16.40.10 mask 255.255.255.255 service snmp

#permit ip-source 172.16.40.10 mask 255.255.255.255 service ssh

#permit ip-source 172.16.40.30 mask 255.255.255.255 service ssh

#deny service telnet

#deny service https

#deny service snmp

#deny service ssh

#exit

#management access-class Hallinta

#exit

6.3.3 HP konfiguraatiot

HP:n laitteet olivat vieraita lukuun ottamatta perinteisiä VLAN-konfiguraatioita. Kyseisestä tuotteesta ei ollut laboratorioon saatavilla laitetta, joten konfiguraatiomanuaaleista tuli selvittää konfiguraatiot AAA-palveluille sekä SSH:lle. Konfiguraatiot noudattivat pitkälti samaa kaavaa kuin Dellin ja Ciscon laitteiden kohdalla. Ensimmäisenä määritellään SSH-palvelut päälle ja luodaan avainparit:

#ssh enable

#ssh port 22

#ssh generate host-key

#ssh generate server-key

HP:n laitteissa tuli varmuuskopiointia varten erikseen ottaa käyttöön vielä *secureco-py*: (SCP)

#ssh scp-enable

#ssh scp-password salasana

Oletuksena HP:n kytkin generoi tunnin välein uuden SSH-avaimen. SSH-avaimen vaihtaminen säännöllisin väliajoin on hyvä, mutta se on järkevää tehdä keskitetysti kaikkiin kytkimiin samalla kerralla. Tästä syystä avaimen automaattinen uudelleengenerointi otettiin pois komennolla:

#ssh interval 0

Varsinaisia AAA-komentoja ei HP:n laitteissa ollut. Laitteisiin määriteltiin TACACS+-palvelin ja muut asetukset hieman eri tavalla. Ensimmäisenä konfiguroitiin tacacs+ -palvelin ja portti:

#tacacs-server primary host 172.16.40.20 key labra

#tacacs-server port 49

#tacacs-server enable

Tämän jälkeen määritettiin, että käytetään Ciscolta tuttua *privilege*-yhdistelmää sekä komentojen valtuuttaminen ja lokitus tapahtui TACACS+-palvelimen avulla:

#tacacs-server privilege mapping

#tacacs-server command-authorization

#tacacs-server command-logging

Lopuksi määriteltiin laitteisiin takaportti eli keino, jolla päästään laitteisiin käsiksi sisäisellä Admin-tunnuksella. Takaportteja oli kahdenlaisia, ”*backdoor*” ja ”secure backdoor” joista valittiin jälkimmäinen käyttöön, sillä se sallii kirjautumisen vain silloin kun TACACS+-palvelin ei ole saatavilla. Kyseinen toiminto suoritettiin komennoilla:

#no tacacs-server backdoor

#tacacs-server secure-backdoor

Laitteille määriteltiin kelloasetukset sillä jokaisen verkon aktiivilaitteen on syytä olla oikeassa ajassa tai ainakin synkronoitu muiden laitteiden kanssa samaan aikaan. Kelloasetukset konfiguroitiin seuraavalla tavalla:

#ntp enable

#ntp primary-server 172.16.40.10

Lopuksi vielä konfiguroidaan hallintaa varten pääsylista, joka sallii ainoastaan liikennöinnin 172.16.40.10 ja 172.16.40.30 IP-osoitteista:

access management-network 172.16.40.10 255.255.255.255

access management-network 172.16.40.30 255.255.255.255

(HP Config Guide 2013)

6.3.4 Varmuuskopiointi ja konfiguraatioiden suorittaminen

Varmuuskopiointi toteutettiin liitteen 7 mukaisella skriptillä eli valmiiksi tehdyllä pienellä ohjelmalla. Varmuuskopiointiin luotiin myös toinen skripti, jonka tehtävänä on ajaa edellä aikaisemmin mainittu skripti automaattisesti, joten se ajastettiin Linuxin crontab-toiminnolla. Näin ollen saatiin aikaiseksi automaattinen varmuuskopiointi. Liitteen 7 ensimmäinen ohjelma ajaa tietyllä käyttäjätunnus-salasana-parilla liitteen 7 toisen skriptin, jossa on itse varmuuskopiointiin tarvittavat tiedot. Koska varmuuskopiointiin ei pystytty olosuhteisiin nähden suunnittelemaan järkevämpää keinoa tuli skriptien käyttöoikeudet suojata mahdollisimman tiukasti (chmod --- <tiedosto>) sekä asettaa käyttäjätunnukselle asetus, ettei tämä saa kirjautua verkkolaitteille kuin crontab-ajastuksen mukaisella ajankohdalla. Toimeksiantajalta tuli pyyntö, että mikäli mahdollista niin ei säilötä muita konfiguraatioita kuin niitä joissa on tapahtunut muutoksia. Skriptiin luotiin kohta, joka vertaa kahta uusinta konfiguraatio tiedostoa toisiinsa ja hävittää uusimman, mikäli sisältö vastaa edellistä. Muussa tapauksessa vanha kopioidaan erilliseen kansioon ja uusi taltioidaan.

Jokaisen laitevalmistajan laitteita on toimeksiantajan verkossa useita, joten on todella työlästä lähteä konfiguroimaan laitteita käsin komento komennolta. Automatisoinnin ollessa alan nykytrendi luotiin toimeksiantajalle skripti jolla komentojen

suorittaminen tietyn laitevalmistajan laitteisiin tapahtuu muutamalla napin painahduksella. Skriptin käyttöliittymän lähdekoodi on esitelty liitteessä 5 kommentteineen. Skriptin perusideana on suorittaa .exp-tiedostojen sisältämiä konfiguraatioita laitteisiin käyttäjän valintojen perusteella. Skriptissä hyödynnettiin koulussa opetettuja eri protokollia kuten SNMP, jonka avulla laitteilta kysyttiin laitevalmistajakohtainen ”System Object ID”. SNMP-kysely on tärkeä, jotta tietyn laitevalmistajan laitteita ei tarvitse sijoittaa omiin tiedostoihinsa vaan ne voivat olla esimerkiksi */etc/hosts*-tiedostossa, jota Linux käyttää niin sanottuna vara DNS-palveluna. Opinnäytteessä tietoturvan ollessa pienessä roolissa oli tärkeää, että käyttöliittymään luotiin kohtia joilla pystyttiin peittämään salasanat ja hävittämään ne käytön jälkeen välimuistista. Käyttöliittymästä pyrittiin tekemään mahdollisimman käyttäjäystävällinen, jonka takia käyttettiin *dialog*-toimintoa skriptissä hyödyksi. *Dialog*-toiminolla voidaan esittää erilasia ikkunoita jossa käyttäjä voi tehdä valintoja, syöttää tietoa tai lukea ilmoituksia. *Dialog*-toiminto on siinä mielessä hyvä, että se voidaan ajaa päätteeltä ilman että käytössä on graafinen työpöytänäkymä. Kuviossa 53 – 57 on esitelty käyttöliittymän erilaisia ikkunoita, joita käyttäjä näkee suorittaessaan skriptiä.

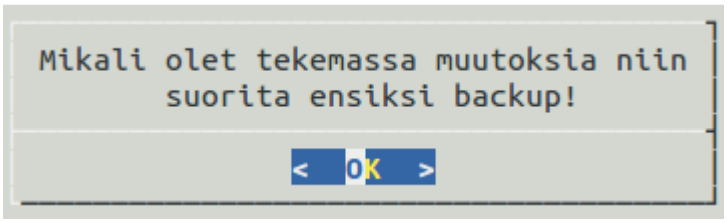
Ensimmäisenä käyttäjältä kerätään tunnistetietoja kuten käyttäjänimi, kuviossa 53 on estitetty käyttöliittymässä esiintyvä ikkuna kyseistä tapahtumaa varten.

KUVIO 53. Selkokielinen käyttäjätunnuksen antaminen

Tietoturvallisuus syistä haluttiin, että salasana pyydetään sillä tavalla, että kirjaimet eivät ole näkyvissä selkokielisenä. Kuviossa 54 on esitetty salasanaikkuna.

KUVIO 54. Ei selkokielinen salasanan antaminen

Käyttäjälle esitetään käyttöliittymässä ilmoituksia, kuten muistutus varmuukopioinnista mikäli tämä on tekemässä muutoksia laitteisiin. Kuviossa 55 on esitetty ilmoitusikkuna.



KUVIO 55. Dialog ilmoitusikkuna

Käyttäjä näkee käyttöliittymässä erilaisia valikoita, joista esimerkkinä valikko jossa valitaan laitevalmistaja joka selvitetään lähdekoodissa SNMP-kyselyn avulla. Edellä kuvattu valikkoikkuna on esitelty kuviossa 56.

KUVIO 56. Päävalikko laitevalmistajan valintaa varten

Edellä mainitun valikon lisäksi käyttöliittymässä valitaan myös suoritettava toiminto samanlaisesta valintaikkunasta. Kuviossa 57 on esitelty tehtävävalikko.

KUVIO 57. Tehtävävalikko haluttua konfiguraatiota varten

Käyttöliittymä on selkeä sekä helppokäyttöinen. HP IMC:n tarjoamat lisäominaisuudet on helppo toteuttaa lisäämällä *.exp*-tiedostoja kyseiseen käyttöliittymään. Näin ollen konfiguraatioiden hallinnan tuoma lisäarvo saavutetaan itse tehdyillä skripteillä.

Dialog-ikkunoiden käyttöön ajatus syntyi netistä löydettyjen tutoriaalien kautta, kuten Jadu Saikan kirjoittaman *”linux dialog utility short turorial”*, joka käsittelee yleisesti dialog-ikkunoiden käyttöä ubuntulla. (Linux dialog utility tutorial 2013)

Skriptit eivät toimi mikäli tyhjä laite asennetaan paikalleen (esim. räkkiin) ja tämän jälkeen ajetaan skriptit. Asennus vaiheessa on asetettava esiasetukset laitteeseen, joita ovat mm. Hallinta VLAN, Hallinta IP-osoite, SNMP-asetukset. Skripti ei ole niinkään uusien laitteiden konfiguroitiin kehitetty, vaikkakin voidaan sitä hyödyntää pienellä jalostuksella myös niihin. Skripti kehitettiin ennemminkin olemassa olevan infrastruktuurin konfigurointiin.

Mikäli Linux-palvelinta käytetään pääteohjelmalla kuten PuTTy, tulee skriptit suorittaa komennolla:

$sudo ./ONT-valikko.sh

Jotta skriptiä ei tarvitse suorittaa pääkäyttäjänä tulee skripti-tiedostoon lisätä suoritusoikeus myös muille käyttäjille komennolla:

$sudo chmod +x ONT-valikko.sh

Koska laboratorioympäristössä oli mahdollisuus käyttää graafista käyttöliittymää, niin haluttiin skriptin käyttö tehdä vieläkin helpommaksi. Näin ollen Ubuntun työpöydälle luotiin kuvion 58 esittämä pikakuvake. Tämän avulla täysin kokematon Linuxin käyttäjä osaa suorittaa skriptin. Pikakuvake luotiin komennolla:

$gnome-desktop-item-edit ~/Desktop/ --create-new

Yllä olevalla komennon jälkeen valitaan *Terminal application* sekä polku jossa skripti sijaitsee.

KUVIO 58. Pikakuvake skriptille

Käyttöliittymän luonnin jälkeen suunniteltiin skriptit joita käytettiin itse aktiivilaitteiden konfigurointiin. Skriptien idea on lyhyesti se, että otetaan yhteys laitteisiin johon käyttäjän tekemät valinnat johtavat. Valintojen jälkeen odotetaan (expect) tiettyä merkkijonoa vastaukseksi ja siihen vastataan lähettämällä (send) ennalta määritetty merkkijono, jota toistetaan niin pitkään kun on tarpeen. Kyseisellä tavalla on helppo konfiguroida olemassa olevia laitteita.

Varmuuskopiointiin piti luoda kaksi skriptiä. Toinen suoritti *.exp*-skriptin ajastetusti tunnuksella, jolla oli oikeus kirjautua laitteisiin ainoastaan tiettynä ajanhetkenä ja suorittaa laitteisiin vain tiettyjä komentoja. Skripti ajastettiin käyttämällä Linuxin crontab-ominaisuutta komennolla:

$sudo vi /etc/crontab

Kuviossa 59 on esitetty crontab-ajastuksen asettaminen komennolle *cd /home/juho/ && ./autobu.sh*, jonka suorittaa käyttäjä *root* ajassa 11.32 aamupäivällä.

```
# m h dom mon dow user  command
17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/c$
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/c$
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/c$
32 11   * * *   root    cd /home/juho/ && ./autobu.sh
#
```

KUVIO 59. Crontab-ajastus

*Crontab*iin on myös mahdollista määrittää *mailto*-ominaisuus, jonka avulla voidaan lähettää ajastuksesta tietoa esimerkiksi palvelimen ylläpidolle.

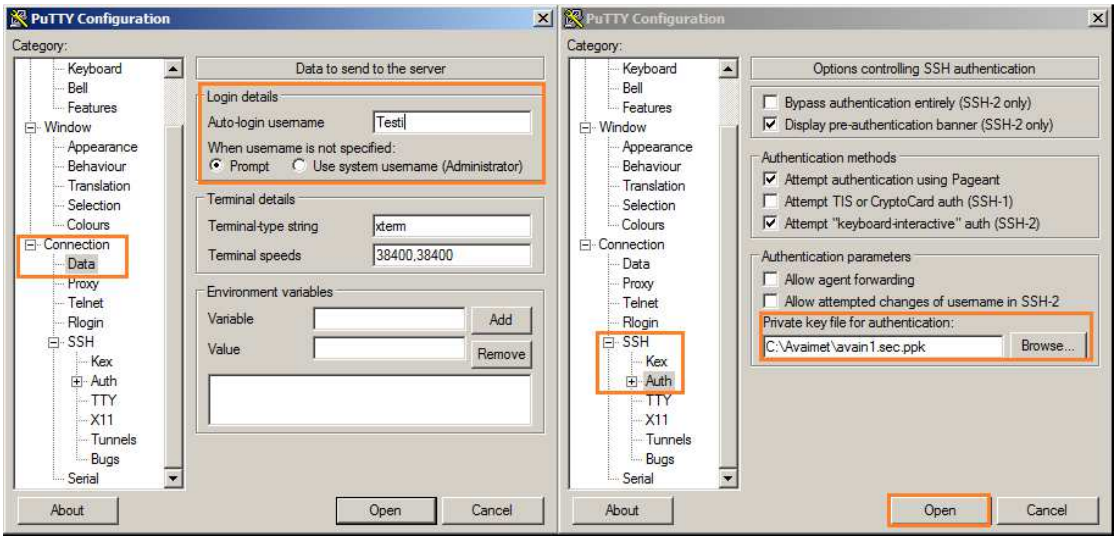
Skripti testattiin myös SLES-palvelimella. Skriptien ideana on se, että ne voidaan implementoida mihin tahansa Linux-koneeseen (Ubuntu, OpenSuse, CentOS yms.) helposti. Pieniä muutoksia kuitenkin pitää skriptiin tehdä, että implementointi onnistuu. *Dialog*-ominaisuuden käytössä on pieniä eroavaisuuksia, *expect*-skriptit toimivat hieman erilailla eri alustoilla ja SNMP-kyselyiden tuottamat tulosteet voivat olla hieman erilaisessa muodossa.

Skriptien jokaisen osa-alueen toiminnan varmentaminen kannattaa aloittaa sillä, että varmistaa että jokainen erillinen lisäosa on asennettu kuten dialog, expect ja niin edelleen.

6.4 VAHTI sisäverkko-ohjeen osa-alueet

Sisäverkko-ohjeen viitteet, joihin opinnäytteessä oli mahdollista vaikuttaa, on listattu liitteessä 8. Viitteet 15.2, 15.12, 15.17, 17.17 ja 17.26 olivat sellaisia, joihin suoranaisesti ei ollut mahdollista vaikuttaa tai ne tulivat käytännössä automaattisesti kuntoon.

Ensimmäinen viite johon työssä pystyttiin vaikuttamaan, oli 15.3. Ensimmäisenä luotiin SSH-kirjautumista varten avainparit PuTTy-keygen ohjelmalla. Ohjelmalla luotiin 2048-bittiset avaimet. Tämän jälkeen julkinenavain siirrettiin käyttäjän *".ssh/authorized_keys"*-tiedostoon. Windowsissa puolestaan avain voi sijaita esimerkiksi käyttäjän omalla verkkolevyllä, joka voidaan määrittää käyttöön PuTTy-pääteohjelmalle kuvion 60 mukaisesti. Kuviossa on myös asetettu kirjautumiseen käytettävä käyttäjänimi, jotta kirjautuminen SSH-palvelimelle onnistuisi mahdollisimman vaivattomasti.



KUVIO 60. PuTTy määritykset

Seuraavaksi varmistetaan, että SSH-palvelimen konfiguraatiotiedostossa *"/etc/ssh/sshd_config"* on seuraavat rivit:

RSAAuthentication yes

PubkeyAuthentication yes

Kielletään kirjautuminen SSH-palvelimelle salasanaa käyttäen. Muokataan edellisen konfiguraatiotiedostoon rivit:

ChallengeResponseAuthentication no

PasswordAuthentication no

UsePAM no

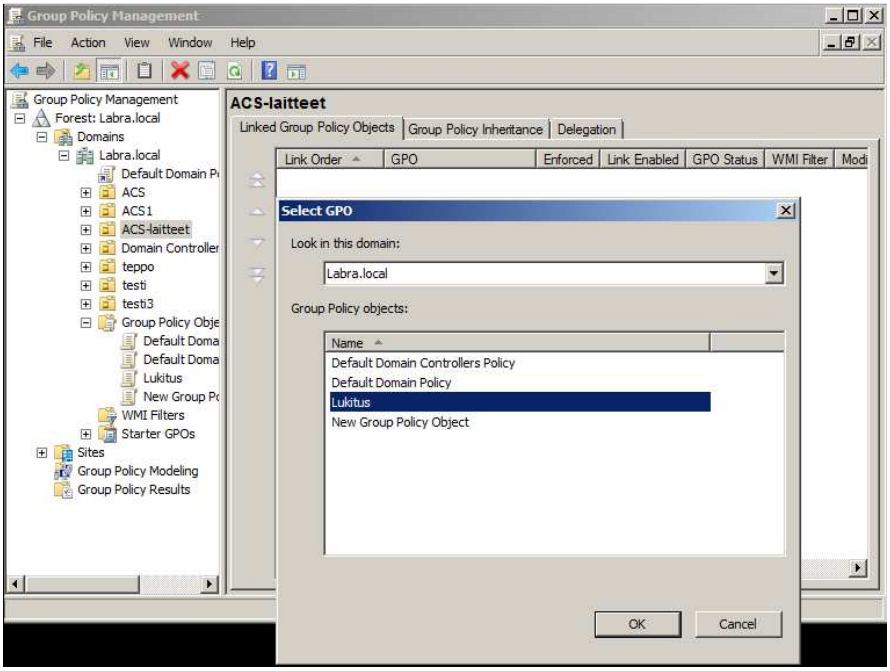
Lopuksi SSH-palvelu pitää käynnistää uudelleen, jonka jälkeen palvelimelle voidaan kirjautua käyttäen avainpareja. Tällä tavalla voidaan hallinta-asemalle pakottaa kirjautuminen avaimeen pohjautuvalla menetelmällä. Lopulta autentikaatioon verkkolaitteille tarvitaan kahta erilaista tunnistusmetodia: "*Mitä tiedät*" ja "*Mitä omistat*". Mikäli tätä tapaa hyödynnetään, niin tulee omasta henkilökohtaisesta salaisesta-avaimesta pitää erityisen tarkkaa huolta.

Kuviossa 61 on esitetty, miltä näyttää kun palvelimelle kirjaudutaan käyttäen SSH-avainta.

```
Using username "root".
Authenticating with public key "imported-openssh-key"
Last login: Sun May  6 09:10:49 2012 from 172.16.40.10
koneA:~ #
```

KUVIO 61. SSH-avaimeen pohjautuva kirjautuminen

Seuraava viite on 15.7 johon yksinkertaisesti luodaan toimenpiteet AD ja ACS-palvelimille. Molemmille palvelimille määritellään, että tunnus lukkiutuu kun käyttäjä on yrittänyt kirjautua esim. 3 kertaa väärällä salasannalla. Kuviossa 62 on esitetty miten kyseinen luodaan AD-palvelimelle.



KUVIO 62. AD GPO

Yllä olevassa kuviossa liitetään ”Group Policy Object” nimeltä ”Lukitus” ACS-laitteet OU:hun, jonka jäsenenä ryhmä ”CiscoACS” on. Ryhmäpolitiikan luomista ei työssä dokumentoida kuvainnollisesti, mutta kyseinen politiikka on luotu ”Group Policy Management Editor”-työkalulla, jossa on muokattu ”Security Settings”-kohtaa ja valittu ”Account lockout threshold” kohdasta ”Properties” ja määritelty kirjautumisyritysten määräksi 3.

Seuraava viite on 15.13 joka tuli lähes automaattisesti hoidettua. Laboratoriossa ACS-palvelimelle kirjauduttaessa ensimmäistä kertaa, pakotti palvelin vaihtamaan salasanan ja muilla tiedonsiirtolaitteilla ei ollut oletustunnuksia. Geneerinen käyttäjätunnus on kuitenkin laitteissa oltava. Tämä mahdollistaa kirjautumisen laitteisiin myös vikatilanteissa.

Seuraava viite on 16.1 jossa käytettiin kahta erilaista ratkaisua. Ensimmäisenä AAA-arkkitehtuuriin liittyvät tapahtuma kirjataan ylös ACS-palvelimelle aiemmin esitetyillä konfiguraatioilla. *Syslog*-tapahtumat, kuten rajapintojen alas/ylösmeno kirjataan erilliselle palvelimelle komennoilla:

Cisco

#logging trap debugging

#logging 172.16.40.10

Dell

#logging 172.16.40.20

#logging file informational

HP

#logging host 1 address 172.16.40.10

#logging host 1 facility

Edellisillä toimenpiteillä saadaan suoritettua myös viite 16.2.

Seuraava viite on 16.4 johon vaikutetaan vaihtamalla salaamaton telnet-protokolla salattuun SSHv2-protokollaan sekä NAS ja ACS-palvelimen välinen tunnistautuminen tapahtuu TACACS+-protokollalla.

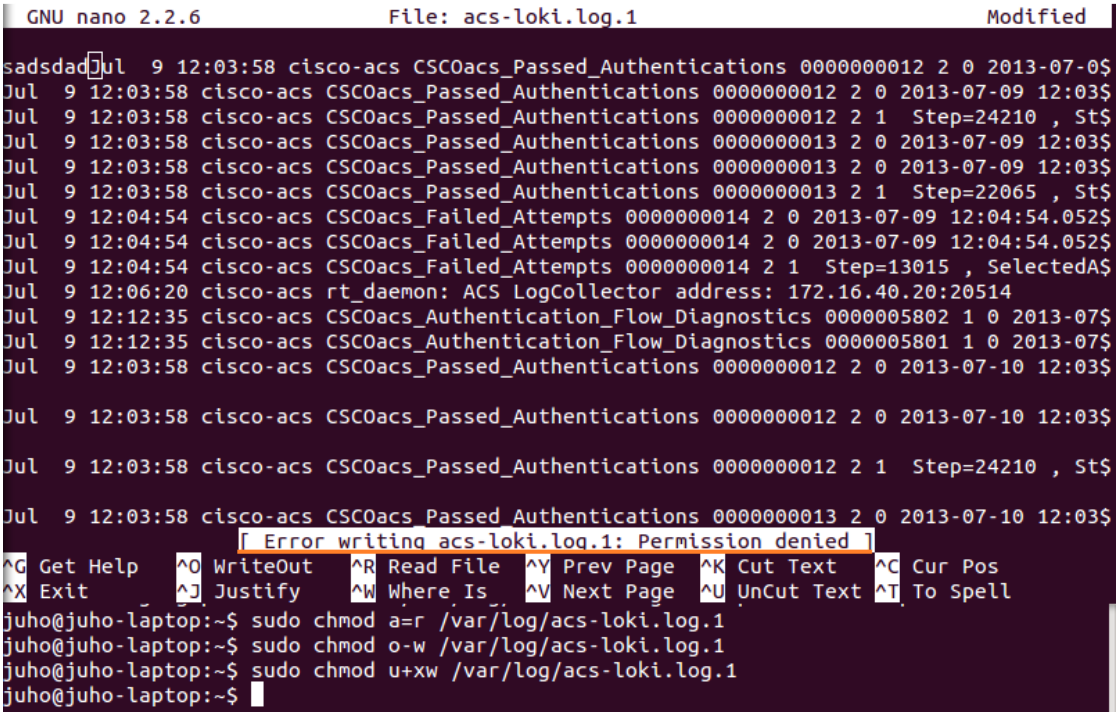
Seuraavana viitteenä on 16.8 johon yksinkertaisuudessaan riittää, että rajataan loki-tiedostojen käyttöoikeudet seuraavilla komennoilla:

$chmod a=r loki.txt

$chmod o-w loki.txt

$chmod u+xw loki.txt

Edellä määriteltiin, että kaikki saavat lukea tiedostoa ”loki.txt” mutta *other*-käyttäjiltä vähennetään kirjoitusoikeus ja omistajalle lisätään kaikki oikeudet. Kyseiset toimenpiteet myös hoitavat osittain viitteen 16.25. Kuviossa 63 on esitelty miten edelliset oikeudet menevät eli kaikki käyttäjät saavat lukea lokeja mutta vain pääkäyttäjät saavat niitä muokata. Tätä voisi vieläkin tiukentaa eli rajata myös lukuoikeudet ainoastaan pääkäyttäjille.



KUVIO 63. Lokitiedostojen kovennus

Seuraava viite on 16.15. *'Audit Trail'* on mahdollista kun verkon aktiivilaitteet on määritetty kirjaamaan komennot ACS-palvelimelle, kuten aikaisemmin konfiguraatioissa on esitelty. Kyseinen tapahtuma on esitelty toimeksiantajalle suunnatun ohjeen loppupuolella liitteessä 3.

Seuraava viite on 16.20, mikä opinnäytteessä suoritettiin sillä, että laboratorioympäristössä oli käytössä erillinen hallinta-asema laitteiden hallintaa varten.

Seuraava viite on 16.24 johon vaikutettiin luomalla hallintaa varten pääsylistat laitteille. Laitteille luotiin pääsylistat jotka myös rajasivat pois sen, että SSH- ja SNMP-protokollat ovat ainoita joita hallintasemalta saa suorittaa laitteille ja muut kontaktiyritykset hallintalinjoihin lokitetaan.

Viite 16.25 tuli osittain hoidettua viitteen 16.8 kohdassa mutta ACS-palvelimelle voidaan vielä rooli määrityksillä määritellä, että valvonta tunnuksilla voidaan ainoastaan selata välilehteä ”Report & Monitoring Viewer”.

Viitteisiin, 17.7, 17.25 ja 17.26 pystyttiin ainoastaan luomaan mahdollisuuksia näiden toteuttamiseen kuten varmuuskopiointiin tarkoitettu skripti sekä ohjeistus siitä, että näin tulisi toimia, jotta tilanteessa missä verkkolaite vaihdetaan esimerkiksi uuteen, ei tulisi ikäviä yllätyksiä.

6.5 AD-palvelimen konfigurointi

Microsoft Windows 2008 r2-palvelimelle oli asennettu aktiivihakemisto-toiminto (active directory), jonka asennusta ei opinnäytetyössä dokumentoida. Kyseiselle palvelimelle tuli kuitenkin tehdä asetuksia, jotka olivat relevantteja työn kannalta. Palvelimelle tuli luoda organisaatioyksikkö (Organization Unit) ja ryhmä (Group). Ryhmä tuli asettaa OU:hun sekä käyttäjät, joille halutaan antaa oikeudet tuli liittää vielä tähän ryhmään. Liitteessä 4 on toimeksiantajalle ohje, jossa tämä tehdään käsin hiirellä klikkailemalla. Kyseisen toiminnon suorittamiseen oli kuitenkin fiksua luoda helpompi tapa. Kyseiset asiat voidaan myös suorittaa komentoriviltä käsin.

Ensimmäisenä luodaan OU AD-palvelimelle:

dsadd ou ou=ACS,dc=Labra,dc=local

Seuraavaksi luodaan ryhmä nimeltä ”ACS-hallinta” joka asetetaan ”Security groupiksi” ja sille määritellään kuvaus sekä liitetään aikaisemmin luotuun OU:hun:

dsadd group cd=ACS-hallinta,ou=ACS,dc=Labra,dc=local –secgrp yes –desc ACS Hallinta ryhmä

Viimeisenä tehdään edellä luotuun ryhmään muutos (modify) ja liitetään valmiina ollut käyttäjä kyseiseen ryhmään:

dsmod group “cn=ACS-Hallinta,ou=ACS,dc=Labra,dc=local” –addmbr “cn=Juho Myllys,cd=Users,dc=Labra,dc=local”

Kun perusasetukset on tehty, on syytä vielä luoda samanlainen komento ACS-palvelimen lisäystä varten:

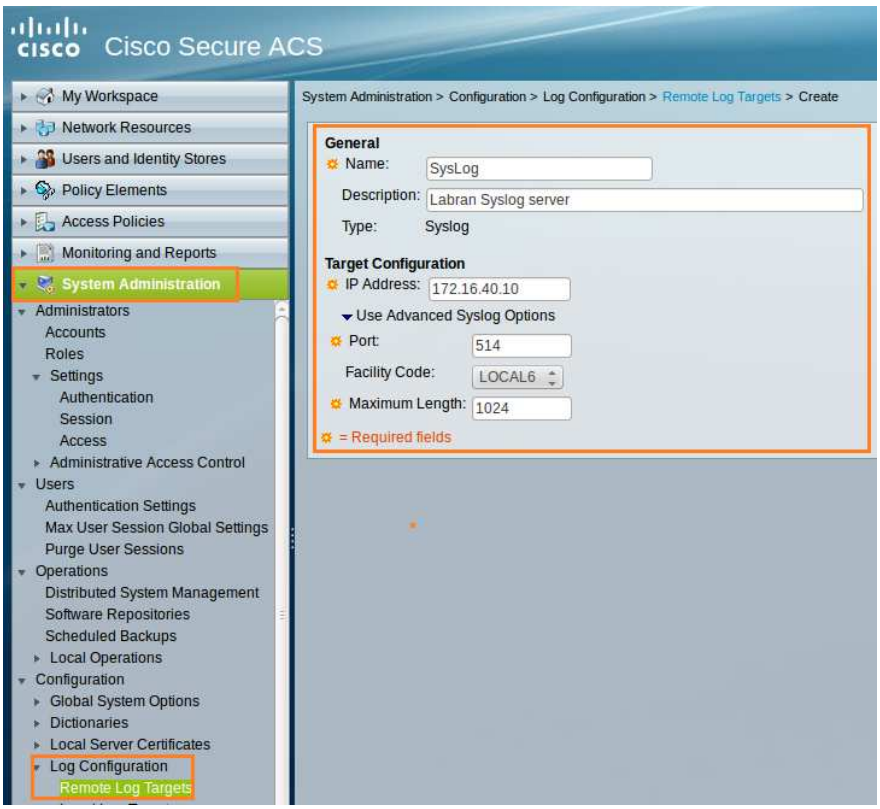
dsadd computer cn=ACS-palvelin1,cn=computers,dc=labra,dc=local –desc ACS-palvelin

Opinnäytetyössä kaikenlainen automatisointi on melko isossa roolissa, joten koettiin hyödylliseksi luoda edellä oleviin toimintoihin Excel-pohja, jonka rakenne ja toiminta on esitelty liitteessä 15.

6.6 Raportointi

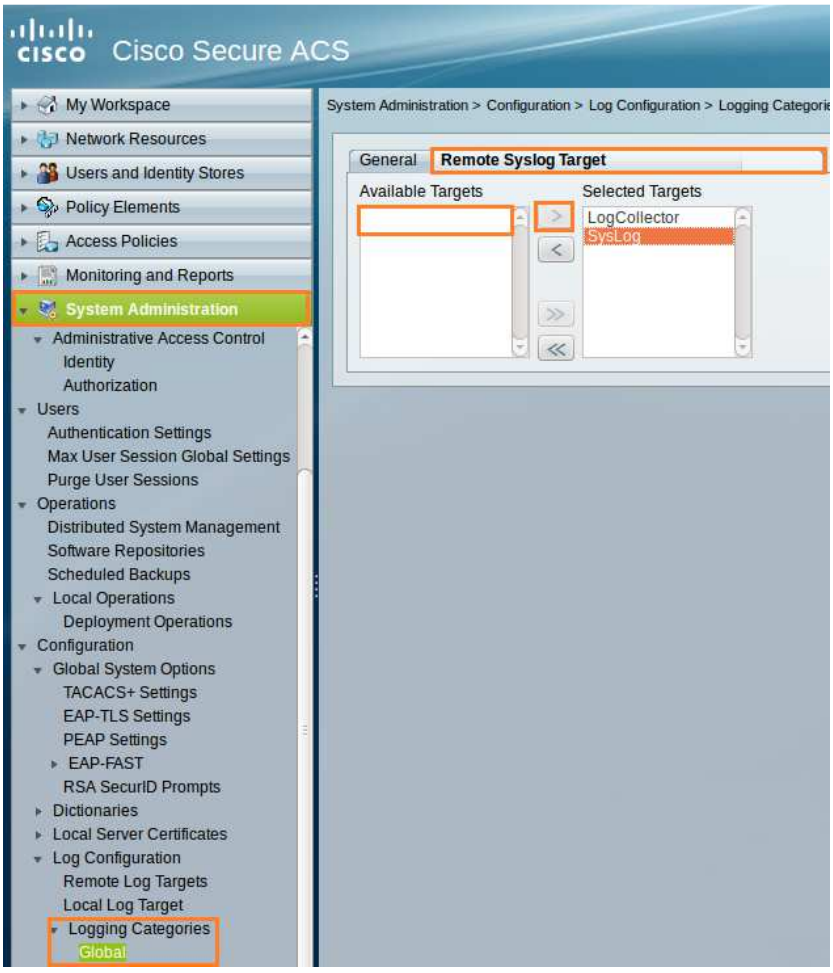
ACS:n toimintaa on syytä välillä seurata vaikka autentikoituminen onnistuisikin moitteettomasti. Tähän on syytä antaa myös mahdollisuus henkilöille joilla ei välttämättä ole tunnuksia ACS-palvelimelle kuten päivystäjille tai tietohallintoon, mikäli näille ei erillisiä tunnuksia luoda. Raportteja voidaan luoda käytännössä mistä tahansa ACS-tapahtumasta, mutta opinnäytteessä dokumentoidaan yksinkertaisin eli autentikointi.

ACS-palvelimelle määritettiin ainoastaan lokitus päälle sekä määriteltiin lokipalvelin, johon ACS-palvelin voi lähettää määritettyjä lokiviestejä. *SysLog*-palvelin määriteltiin kuvion 64 mukaisesti.



KUVIO 64. SysLog-palvelimen määrittäminen ACS–palvelimelle

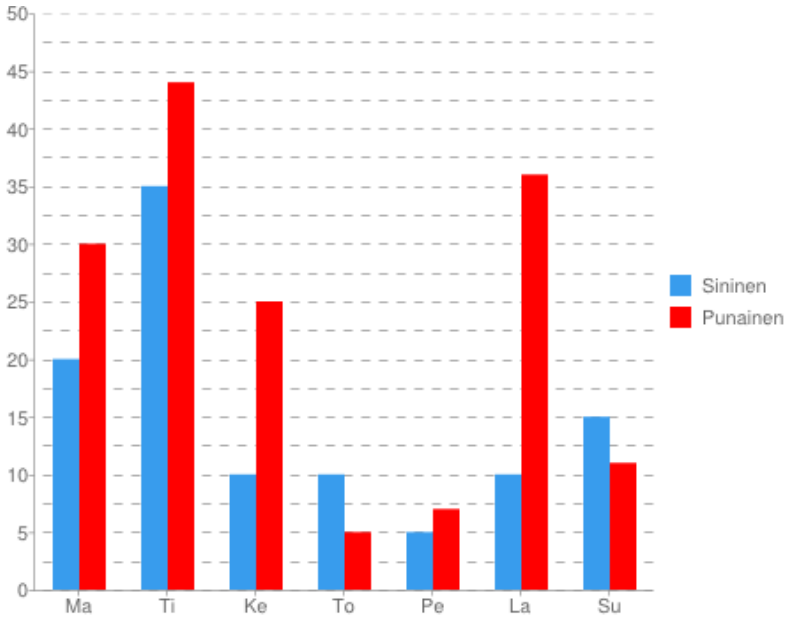
ACS-palvelinta tutkiessa tuli eteen ongelma, johon ei opinnäytetyössä keksitty ratkaisua mutta ongelma pystyttiin kiertämään pienellä ylimääräisellä työllä. ACS-palvelimen asetuksista ei löytynyt kohtaa, jossa lokiviestien aikaleiman voisi vaihtaa sellaiseksi, joka olisi mahdollistanut viikonpäivän näkymisen SysLog-viesteissä. Liitteessä 16 eli raporttien luomiseen käytetyssä lähdekoodissa on luotu omat muuttujat viikonpäiville, joiden avulla pystyttiin liittämään onnistuneet ja epäonnistuneet autentikaatiot oikeille päiville. Muuttujat ovat luotu sillä olettamuksella, että skripti ajetaan joka sunnuntai. SysLog-palvelimen asettamisen jälkeen tuli palvelimelle vielä konfiguroida, että mitä viestejä ACS-palvelimen halutaan lähettävän SysLog-palvelimelle. ACSn toimiessa suuressa tuotantoympäristössä syntyy lokia aivan käsittämätön määrä. Laboratorioympäristössä haluttiin rajata viestien määrää mahdollisimman alhaiseksi selkeyden vuoksi. Seuraavassa kuviossa 65 on esimerkki siitä miten ACS–palvelimelle voidaan asettaa haluttuja tapahtumia lokitettavaksi.



KUVIO 65. ACS-lokitapahtumien määrittely

Yllä olevassa kuviossa on valittu *”Available Targets”*-kodasta, aikaisemmin luotu Sys-Log-palvelin ja vaihdettu se *”Selected Targets”*-kohtaan. Luotu SysLog-palvelin on oletuksena jokaisessa osiossa *”Available Targets”*-kohdassa, joten ilman määrittelyjä ei lokipalvelimelle lähetetä viestejä. *”System Administrator”* → *”Logging Categories”* → *”Global”*-lehdestä täytyy vielä valita haluttu lokitapahtuma, kyseinen osio ei näy kuviossa 65. Tapahtumia on todella laaja skaala joten on syytä harkita, minkälaista näkyvyyttä halutaan saada ACS-palvelimelta ulospäin.

Raporttien osalla opinnäytetyössä hyödynnettiin Googlen palvelua nimeltä *”Chart”*. Kyseisen palvelun avulla voidaan luoda erilaisia kuvaajia kuvaamaan lähes mitä tahansa tapahtumaa. Kuvaajan luontia varten tarvittavat tiedot ovat täysin riippuvaisia käyttöön halutusta kaaviotyypistä ja siitä, että minkälaisia tietoja kaavioon halutaan. *”Chart”*-toiminto toimii sillä tavalla, että URL-kenttään syötetään osoite, joka pitää sisällään halutut tiedot. Kyseisten tietojen perusteella Googlen palvelimella muodostetaan sitten kuvaaja, joka palautetaan web-sivustolle näkyviin. Kuviossa 66 on esitetty esimerkki kuvaaja.



KUVIO 66. Google Chart Kuvaaja

URL jonka avulla on luotu edellä oleva kuvaaja, on seuraavanlainen:

https://chart.googleapis.com/chart?cht=bvg&chs=450x350&chd=t:20,35,10,10,5,10,15|30,44,25,5,7,36,11&chxr=1,0,50&chds=0,50&chco=389ced,FF0000&chbh=15,0,20&chxt=x,y&chxl=0:|Ma|Ti|Ke|To|Pe|La|Su&chdl=Sininen|Punainen&chg=0,5,5,5

URL-muuttujaan määritetään kuvaajan tyyppi eli *”cht”*, kuvaajan koko *”chs”*, kuvaajan tiedot *”chd”* eli eri muuttujien (Sininen ja Punainen) arvot kuhunkin pystysarakkeeseen, kuvaajan nousutaso *”chxr”* eli yhden välein nousee 0 – 50 akselilla, kuvaajan pystyakseli skaalaaja *”chds”* eli 0 – 50 on akselinkorkeus, akseleiden värit *”chco”*, palkkien asetukset *”chbh”* eli kuinka leveitä, kaukana toisistaan (vierekkäiset) ja kuinka kaukana toisistaan ”0” – akselilla palkit ovat ja loppuun määritellään akselit (x ja y) *”chxt”* sekä *”chxl”* joista jälkimmäisen perään määritellään vaaka-akselin tiedot ja viimeisenä tulee pystypalkkien nimet *”chdl”* ja poikkiviivojen säädöt *”chg”*.

Kaavio on huomattavasti käyttäjäystävällisempi tapa seurata esimerkiksi viikoittaisia autentikaatiotapahtumia yleisesti. Tämä on toki myös mahdollista myös ACS-palvelimella, mikäli käyttäjällä on tunnukset. Yksityiskohtaista tietoa kuitenkaan tässä ratkaisussa ei voida tietoturvasyistä käyttää mutta yleistä ”trendiä” voidaan seurata.

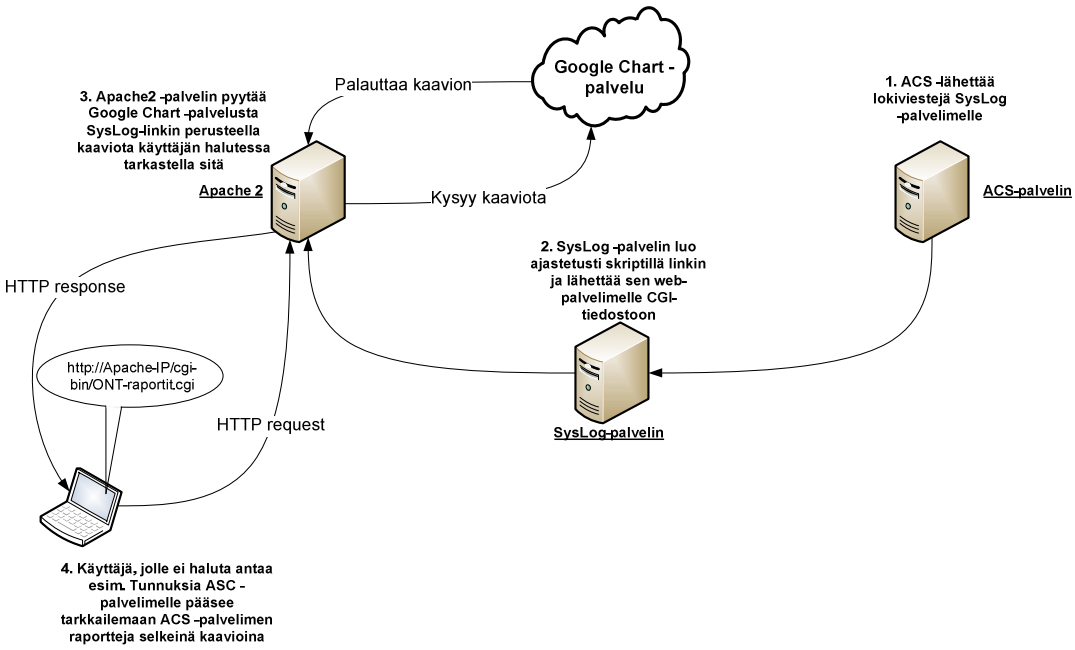
Mikäli kaaviota halutaan hyödyntää oikeasti, tulee ACS-palvelimelta tulostaa autentikaatio-lokitietoja ulkoiselle palvelimelle (SysLog), jossa automaattinen skripti luo raportointi tiedostoon URL:in jonka kopioimalla päästään katsomaan viikkotasolla esimerkiksi onnistuneita ja epäonnistuneita autentikaatiota. Vaikka kaavio luodaan Googlen-palvelun kautta, ei liikenteen seassa ole mitään oleellista tietoa, sillä kaaviot eivät sisällä kuin ”AuhtOk” ja ”AuthFail”-nimet, joista ei vielä paljoa voida päätellä. Liikennöintiin käytetään HTTPS-protokollaa, joka mahdollistaa suojatun tiedonsiirron. Googlen palvelu mahdollistaa myös levytilan säästämisen, sillä URL tekstimuodossa ei vie käytännössä yhtään levytilaa.

Kaavioita on syytä käydä kuitenkin silloin tällöin läpi, jotta voidaan havaita, mikäli autentikaatioissa on havaittavissa poikkeamia. Skripti joka luo URL:t on esitetty liitteessä 16.

Raporttien seuraaminen on yksinkertaista, osoitteet kopioidaan määritellystä tiedostosta ainoastaan WWW-selaimen osoitekenttään ja painetaan *enter*-näppäintä ja

haluttu kaavio latautuu näkyviin. Kaaviota kopioidessa on kuitenkin syytä huomata, ettei kopioida kaavion loppu osaa ”.päivämäärä_viikko”, joka on lopussa sitä varten, että voidaan valita viikkonumeron tai kopiointi päivämäärän perusteella sopiva raportti tarkasteluun.

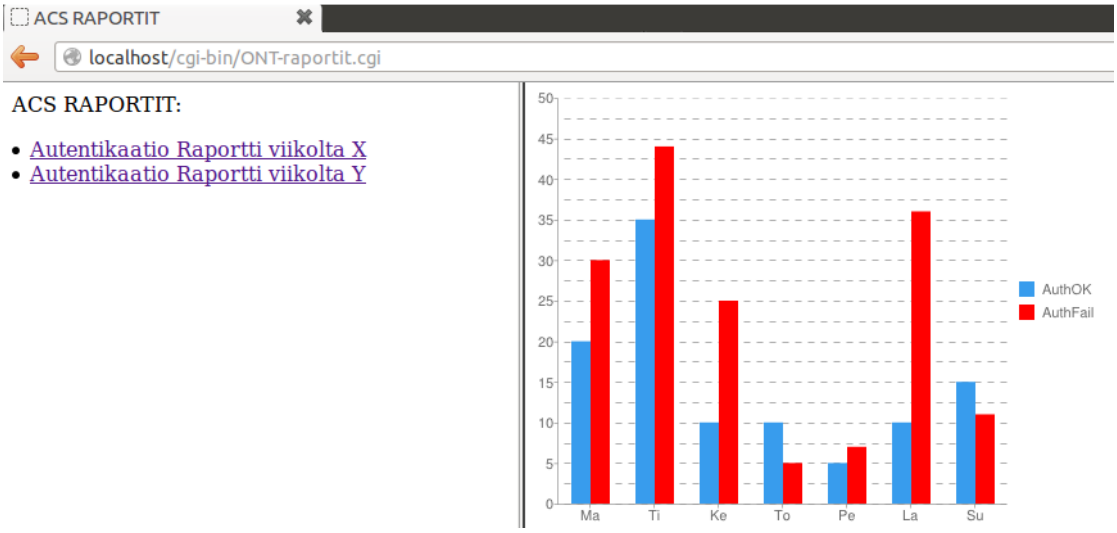
Edellä esitettyä tapaa miettiessä, havaittiin kaavioiden tarkastelu kankeaksi, käyttämällä kopioi ja liitä-menetelmää. Näin ollen pienellä lisäsuunnitellulla luotiin tapa, jolla käyttäjät voivat tarkastella raportteja yhdeltä WWW-sivulta. Raporttien luomisessa käytetty periaate on esitelty kuviossa 67. Huomioitavaa kuviossa on kuitenkin se, että Apache 2- ja SysLog–palvelin ovat fyysisesti samaa palvelinta, mutta havainnollistamisen vuoksi ne eroteltiin kuvioon.



KUVIO 67. Raporttien luomiseen käytetty periaatekuvio

Koska opinnäytetyössä raportointi osiossa hyödynnettiin Googlen tarjoamaa palvelua, säästyttiin kompleksisemmalta kokonaisuudelta ja vältyttiin esimerkiksi tietovaraston pystyttämiseltä johon kaaviot voidaan tallentaa sekä kaavioiden luomiselta käsin. Yksi huomion arvoinen asia on, että *Apache 2*-palvelimen tulee olla yhteydessä julkiseen verkkoon tai ainakin sen kautta Google Chart-palveluun.

Seuraavassa kuviossa 68 on esitelty miltä Web-sivusto näyttää, jossa raportteja voidaan tarkastella. Kuvioon on lisätty käsin kyseiset kaaviot ja SysLogeja on manipuloitu, jotta kaaviot näyttävät muutakin kuin muutamia onnistuneita autentikaatiota.



KUVIO 68. Web-sivu ACS-raporteille

Raportointiin tarvittavat tiedostot on esitelty liitteessä 16 lähdekoodeineen.

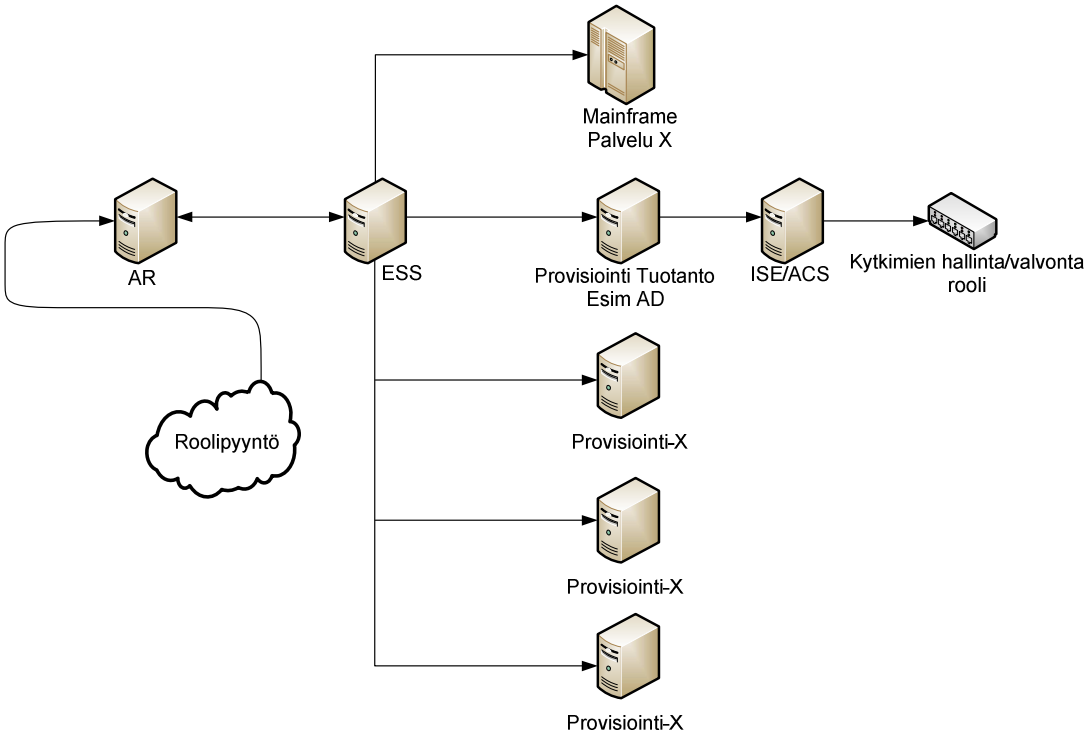
6.7 Käyttövaltuuksien hallinta

Opinnäytetyössä suurena osana oli aiheen kokonaisvaltainen suunnittelu. Tästä syystä tuli ottaa huomioon käyttövaltuuksien hallinta. Suuressa organisaatiossa jossa on paljon eritasoisia osastoja, ei voida oikeuksia antaa mielivaltaisesti kenelle tahansa, mihin tahansa kohdesovellukseen tai järjestelmään. Toimeksiantajalla oli olemassa oleva järjestelmä käyttövaltuuksien anomiseen sekä niiden myöntämiseen.

Toimeksiantajan käyttövaltuutus järjestelmä

Toimeksiantajan työntekijöiden perustietoja hallinnoidaan sille varatussa järjestelmässä, josta ne välittyvät käyttövaltuuksien hallintajärjestelmään. Työntekijöiden esimies myöntää alaisilleen tehtävien mukaiset käyttövaltuudet KVH-järjestelmässä (Käyttövaltuushallinta), josta ne välitetään automaattisesti kohdejärjestelmiin. Käyttövaltuuksia ei kirjata siis käsin suoraan kohdejärjestelmiin kuten opinnäytetyössä

ACS-palvelimelle tai tarkemmin ottaen AD-palvelimelle, vaan kaikki pyörähtää KVH-järjestelmän kautta. Käyttövaltuusroolit voidaan määritellä yksittäiseksi rooliksi tai/ja vaihtoehtoisesti kuuluvaksi tehtävärooliin. Normaalirooli voi antaa oikeudet joko yksittäiseen sovellukseen kuten työssä kytkimien hallinta tai vaihtoehtoisesti useampaan sovellukseen. Tehtäväroolit pitävät puolestaan sisällään useita perusrooleja. KVH-järjestelmä on kuvattu perustasolla kuviossa 69.

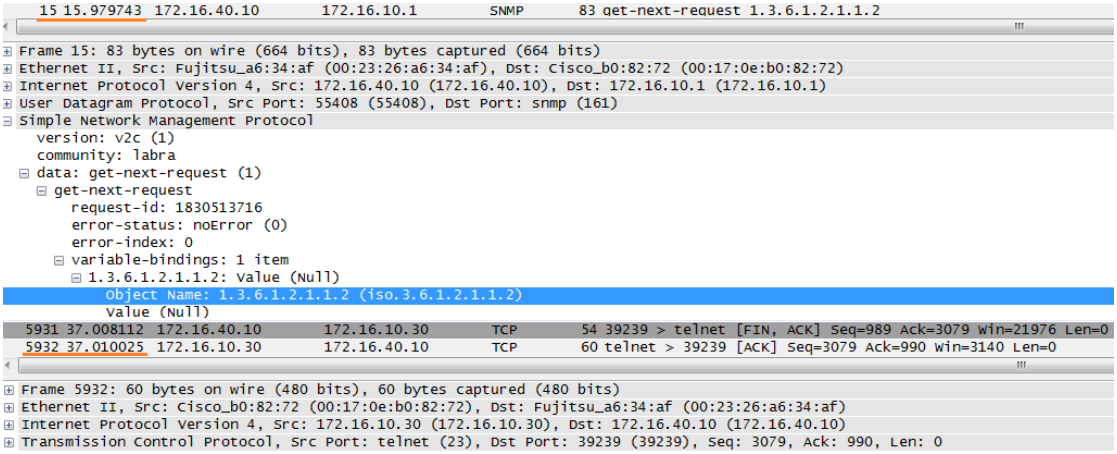


KUVIO 69. Käyttövaltuusjärjestelmä

Edellä olevaan järjestelmään opinnäytetyössä uutena osana suunniteltiin AD-järjestelmän alle ISE/ACS-rooli, jota anomalla pystytään anomaan käyttövaltuuksia kytkimien hallintaan/valvonta rooliin. Prosessi etenee sillä tavalla, että roolin anominen kohdejärjestelmään lähetetään ensimmäisenä AR-palvelimelle (Action Request Server), josta anomus menee ESS-palvelimen (Enterprise SecurityStation) kautta kohde järjestelmän provisiointi moduulille jossa käyttäjän pyytämä rooli automatisoidaan käyttäjän käyttäjätiliin, mikäli se on hyväksytty. Kyseinen tapa säästää työaikaa ja IT-osastolla työskentelevien asiantuntijoiden ei tarvitse tehdä manuaalisesti liitoksia roolien ja käyttäjätilien välille.

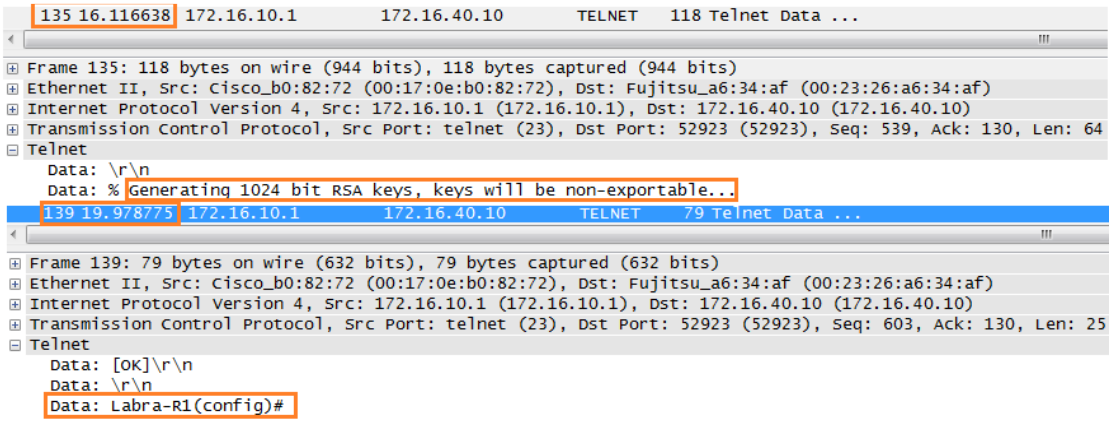
7 TULOKSET

Laitteiden konfigurointi lähti liikkeelle sillä, että laitteisiin oli aikaisemmin konfiguroitu konfiguraatiot jotka muistuttavat tilannetta joka voisi olla jo tuotannossa eli VLANit, portit ja niin edelleen. Ensimmäisenä laitteisiin konfiguroitiin SSH ja AAA-asetukset skriptin avulla. Kuviossa 70 on esitetty WireShark kuvakaappaus, jossa on otettu ensimmäisestä SNMP-kyselystä viimeisen TCP-istunnon lopetusviesteihin (FIN, ACK & ACK) asti talteen.



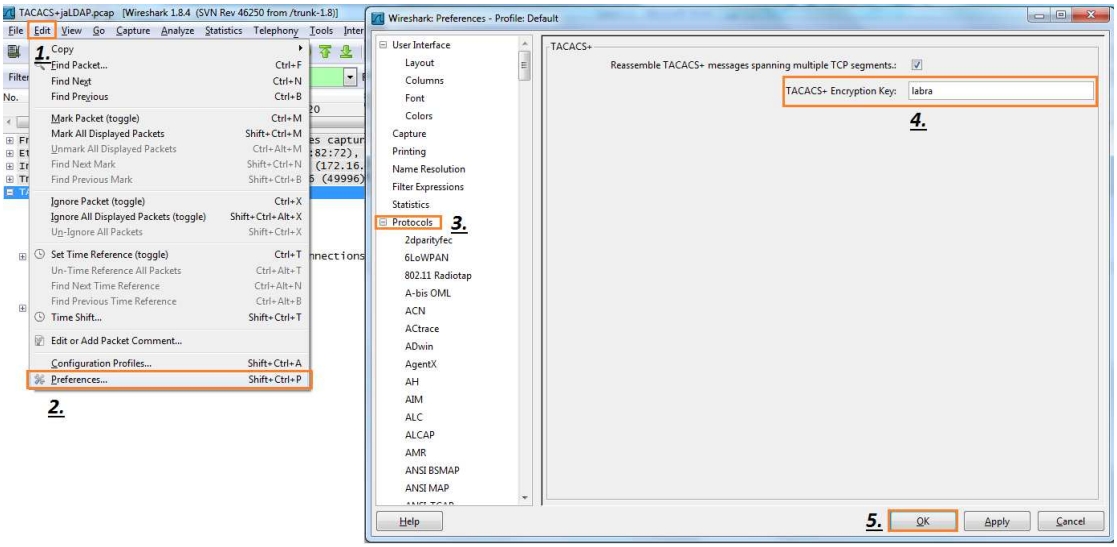
KUVIO 70. Skriptin aloitus ja lopetus

Kuten edellä olevasta kuviosta voidaan havaita, on paketteja liikkunut lähes 6000 kappaletta. Huomioitavaa kuitenkin tässä on se, että aikaa on kulunut ensimmäisestä SNMP-kyselystä viimeisen Ciscon laitteen konfiguroinnin lopettamiseen ainoastaan noin 21 sekuntia. Verkkolaitteita jotka konfiguroitiin olivat Labra-r1, Labra-sw1 – 3 eli 4 verkkolaitetta. Jokaiseen laitteeseen generoitiin RSA-avaimet, joiden luomiseen kului kuvion 71 mukaisesti hieman alle 4 sekuntia. Joten itse konfiguraatio tapahtui todella nopeasti ottaen huomioon neljän RSA-avaimen luomisen ja kokonaisajan.



KUVIO 71. RSA-avainparin luomiseen kuluva aika

Konfiguraatioiden ja ACS-palvelimen pystytyksen jälkeen testattiin kirjautumista verkkolaitteelle tilanteessa, jossa ACS-palvelimelle oli määritelty käyttöön AD-palvelimen käyttäjätietokanta. Kirjautumista todennettaessa, ensimmäisenä selvitettiin kuinka WireShark-ohjelmistolla saadaan paketeista mahdollisimman paljon tietoa. WireShark-ohjelmistoon sai määriteltyä TACACS+-protokollan salausavaimen kuvion 72 mukaisella tavalla.



KUVIO 72. TACACS+ -protokollaan salausavaimen syöttäminen

Kolmanteen kohtaan tarkennuksena se, että ”Protocols”-kohdasta etsitään TACACS+. Mikäli salausavain joka syötetään kohtaan 4, on oikea, niin WireShark-ohjelmistoon muodostuu TACACS+-kenttien alle ylimääräinen kenttä ”Decrypted Request/Reply”,

josta nähdään selkokielisinä mm. käytetyt attribuutit. Esimerkki selkokielisestä osuudesta on esitetty kuviossa 73.

```
Decrypted Request
    Action:
    Privilege Level:
    Authentication type:
    Service:
    User len:
    User:
    Port len:
    Port:
    Remaddr len:
    Remote Address:
    Data:
```

KUVIO 73. TACACS+ Decrypted Request

Käyttäjän kirjautuminen aktiivilaitteelle alkaa siitä kun NAS-laite lähettää TCP SYN-viestin ACS-palvelimelle, joka on esitelty kuviossa 74.

```
Internet Protocol Version 4, Src: 172.16.10.1 (172.16.10.1), Dst: 172.16.40.20 (172.16.40.20)
Transmission Control Protocol, Src Port: 49996 (49996), Dst Port: tacacs (49), Seq: 0, Len: 0
    Source port: 49996 (49996)
    Destination port: tacacs (49)
    [Stream index: 1]
    Sequence number: 0    (relative sequence number)
    Header length: 24 bytes
    Flags: 0x002 (SYN)
```

KUVIO 74. TACACS+-palvelimelle TCP SYN-paketti

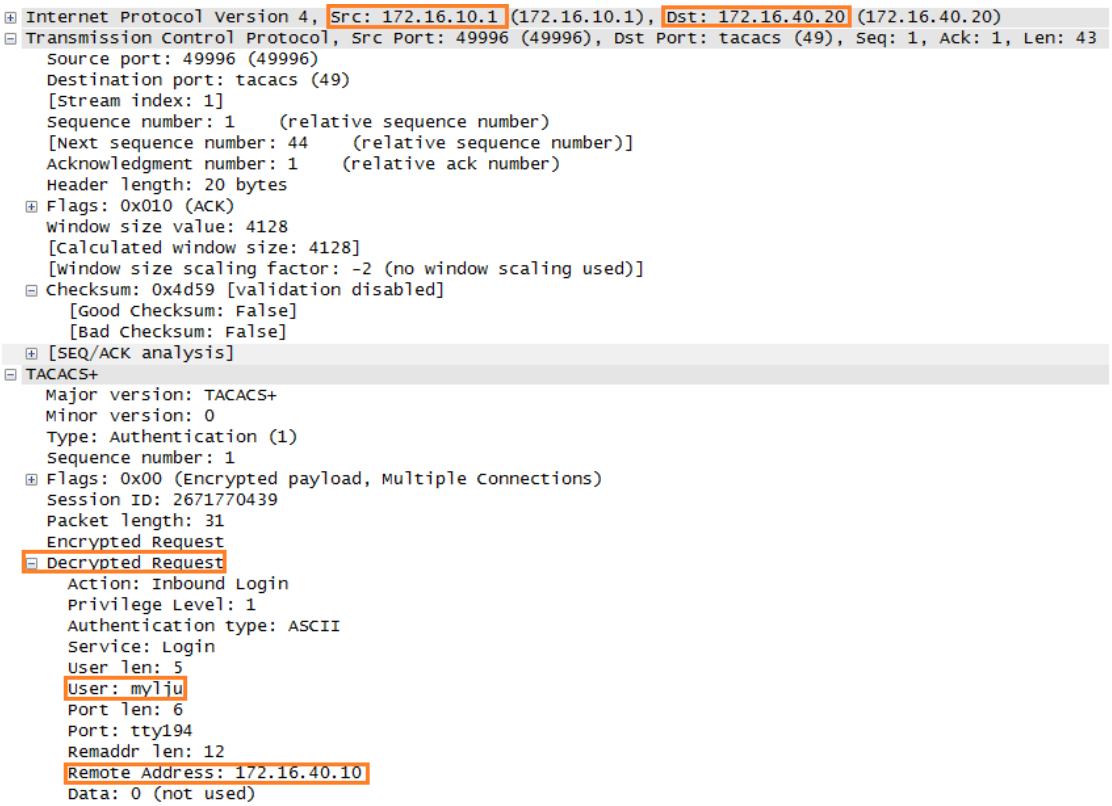
Tähän pakettiin ACS-palvelin vastaa TCP SYN ACK-viestillä, mikäli kaikki on kunnossa. Kuviossa 75 on palvelimelta saapunut TCP SYN ACK-viesti NAS-laitteelle.

```
Internet Protocol Version 4, Src: 172.16.40.20 (172.16.40.20), Dst: 172.16.10.1 (172.16.10.1)
Transmission Control Protocol, Src Port: tacacs (49), Dst Port: 49996 (49996), Seq: 0, Ack: 1, Len: 0
    Source port: tacacs (49)
    Destination port: 49996 (49996)
    [Stream index: 1]
    Sequence number: 0    (relative sequence number)
    Acknowledgment number: 1    (relative ack number)
    Header length: 24 bytes
    Flags: 0x012 (SYN, ACK)
```

KUVIO 75. NAS-laitteelle TCP SYN ACK paketti.

NAS-laite kuittaa lopuksi viestin ACK-viestillä.

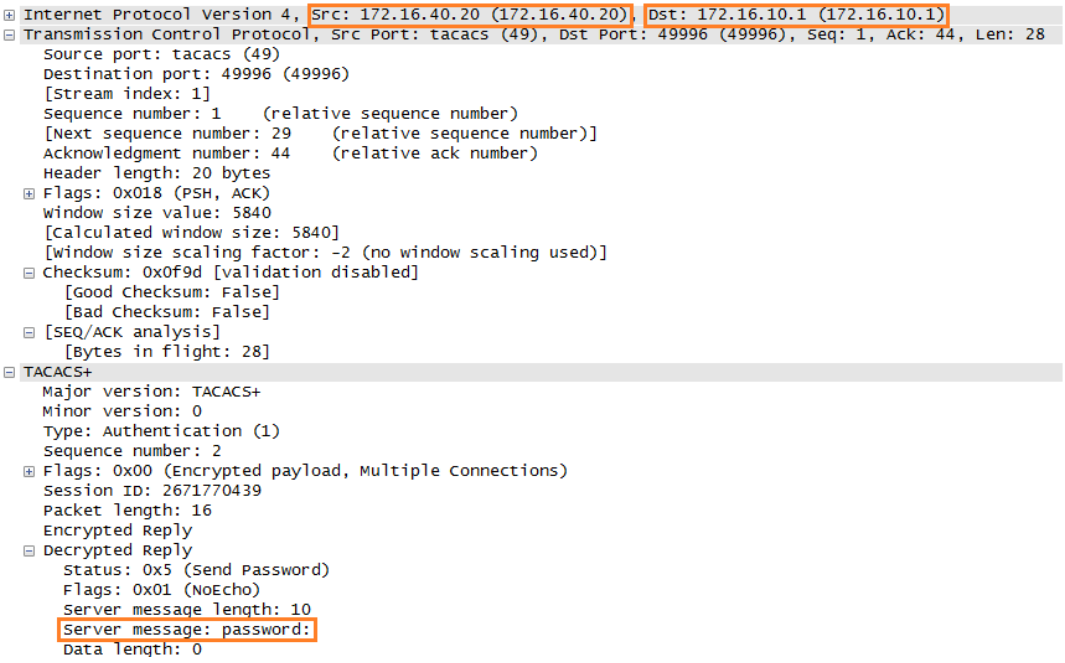
Seuraavaksi aloitetaan autentikointiprosessi lähettämällä käyttäjän syöttämä käyttäjänimi TACACS+-pakettina ACS-palvelimelle. Kuviossa 76 on TACACS+-paketti, joka on purettu auki (decrypt) WireShark-työkalulla. Merkkijono ”User:” ei tarkoita käyttäjätunnusta, vaan että käyttäjä on kirjoittanut viestiin jotain. Vastaavasti palvelimen lähettäessä tekstiä on merkkijonona ”Server message”.



KUVIO 76. TACACS+ -autentikaatioviesti

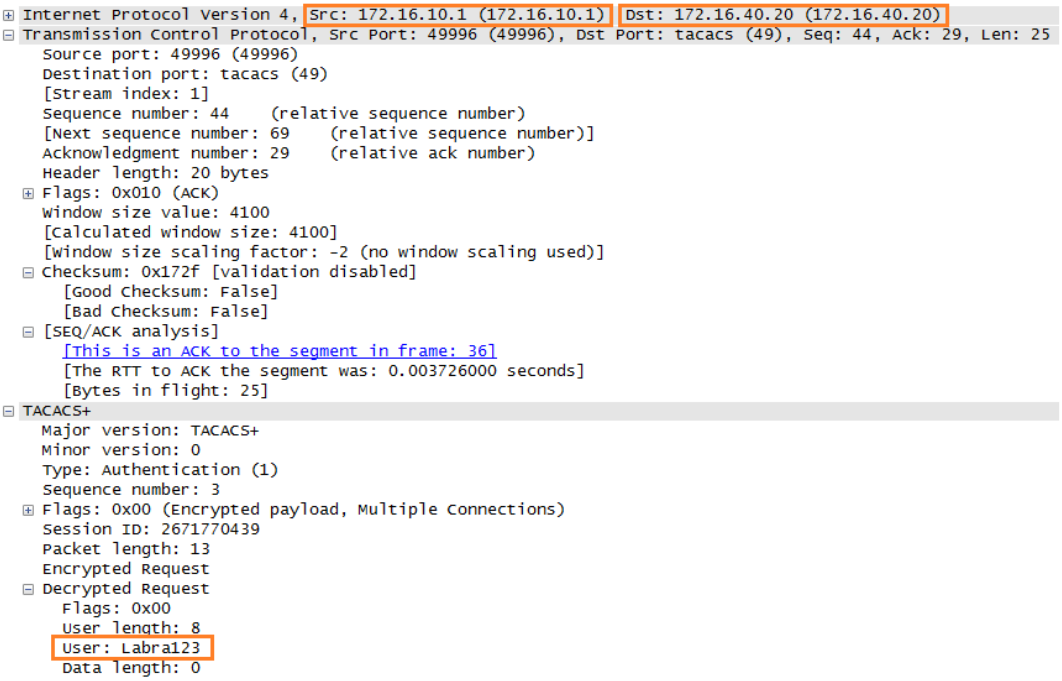
Edellisessä kuviossa on rajattu oranssilla värillä oleellisia asioita kuten NAS-laitteen IP-osoite (src) ja ACS-palvelimen IP-osoite (dst). Kuviosta voidaan myös havaita, että TACACS+-paketti sisältää salaamattoman osion. josta voidaan todentaa TACACS+ -protokollan toimintaa ja attribuutteja.

Edellisen autentikaatioviestin TACACS+-palvelin kuittaa TCP ACK-viestillä, jonka jälkeen se lähettää käyttäjälle tiedustelun salasanasta. Kuviossa 77 on purettu TACACS+-paketti, jossa on näkyvissä salasana kysely.



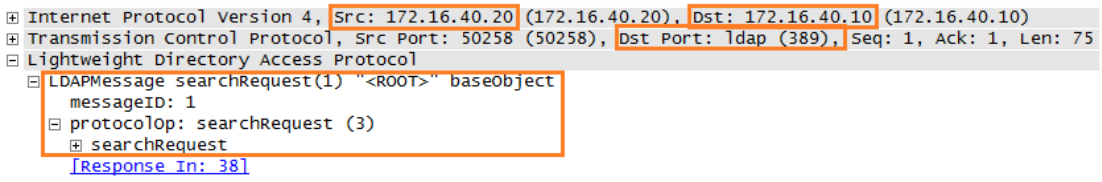
KUVIO 77. TACACS-palvelimen salasanakysely

Tämän viestin käyttäjä kuittaa syöttämällä merkkijonon päätteelle ja hyväksymällä sen painamalla *enter*-painiketta. Kuviossa 78 on paketti, johon käyttäjä on syöttänyt salasanansa vastatakseen TACACS+-palvelimen lähettämään salasana kyselyyn.



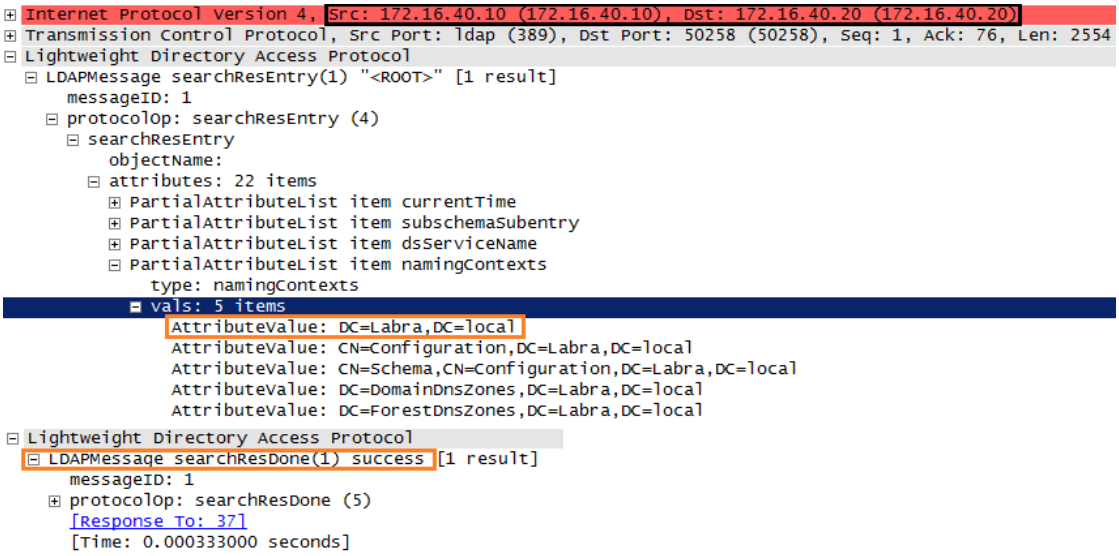
KUVIO 78. Käyttäjän syöttämä salasana TACACS+ -palvelimelle

Jälleen TACACS+-palvelimen tulee kuitata käyttäjän lähettämä viesti ACK-viestillä. Ennen kuin TACACS+-autentikaatio viedään loppuun, tulee ACS-palvelimen etsiä käyttäjä AD-palvelimelta käyttäen LDAP-protokollalla ja tunnistaa käyttäjä kerberos-todennusprotokollalla. Testejä yksinkertaistaessa kirjauduttiin AD-palvelimelta laitteisiin. Tästä syystä WireShark kuvakaappauksissa IP-osoitteet menevät hassusti, käyttäjän ”Remote Address” on sama kuin IP-osoite, johon ACS-palvelin lähettää LDAP-kyselyt. ACS-palvelin lähettää LDAP-kyselyn AD-palvelimelle, johon AD-palvelin tulee vastata. Kuviossa 79 on tapahtuma jossa ACS-palvelin avaa yhteyden LDAP-palvelimelle, joka on määritelty ACS-palvelimelle ulkoiseksi käyttäjätietokannaksi (Active directory).



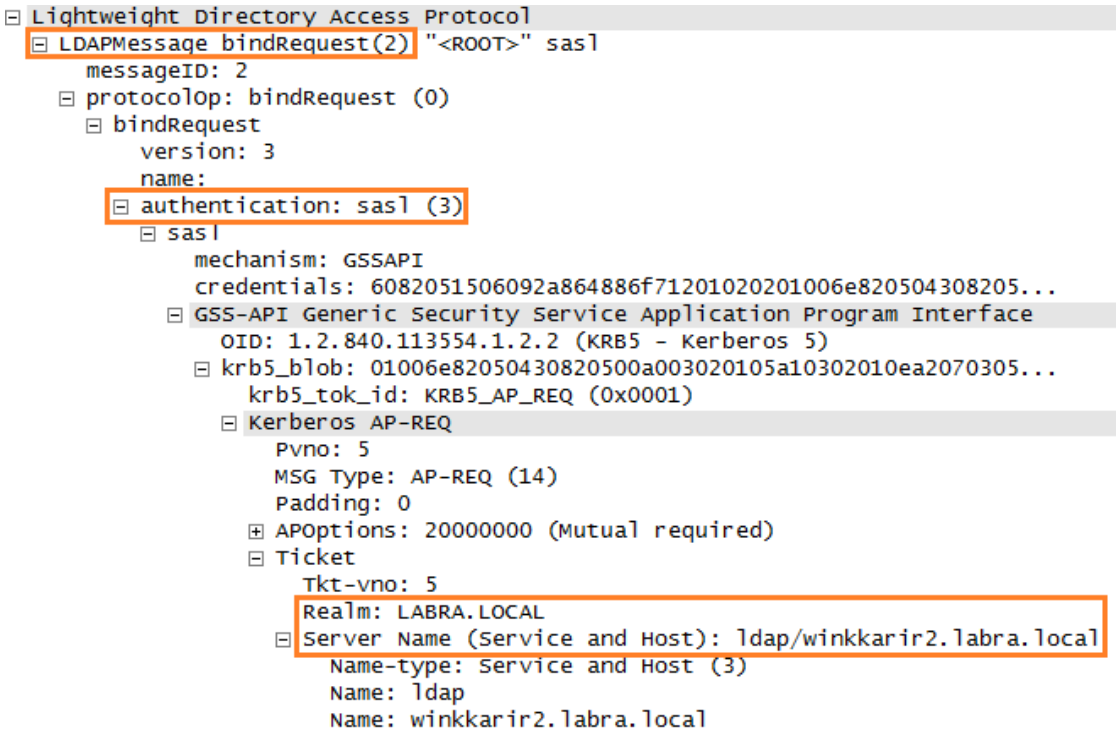
KUVIO 79. LDAP SearchRequest

Edelliseen viestiin AD-palvelin vastaa LDAP ”searchResEntry”-viestillä, jonka mukana lähetetään myös viesti ”searchResDone”. Vastaus kertoo löydetyt tulokset ja sen, että etsintä on valmis. Kuviossa 80 on esitelty, että LDAP löytää esimerkiksi oikean toimi alueen ja kuviosta havaitaan myös, että etsintä on valmis.



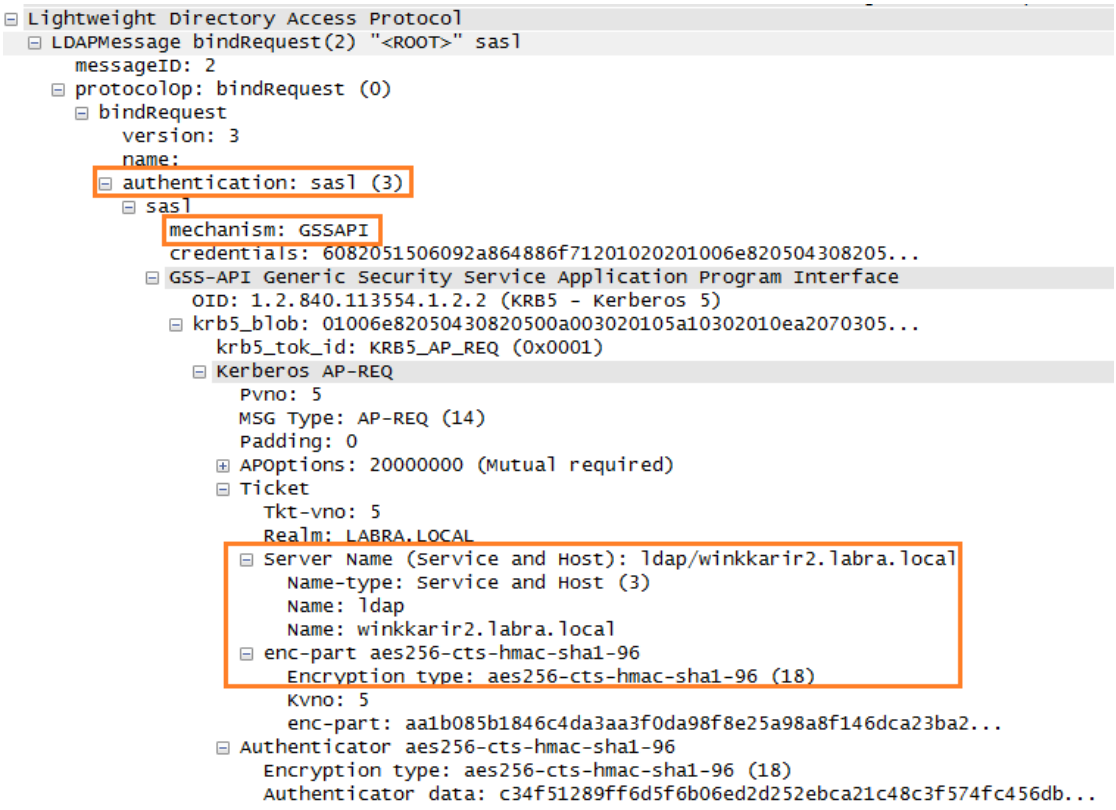
KUVIO 80. LDAP Search-vastaukset

Seuraavaksi ACS-palvelin lähettää AD-palvelimelle ”bindRequest”-viestin. Tämän viestin tehtävänä on haastaa AD-palvelin tiettyyn autentikaatio tasoon. Näiden viestien avulla sovitaan yhteisistä autentikaatiotavoista. Kuviossa 81 on LDAP ”bindRequest”-viesti, josta nähdään autentikaatiometodi sekä sen salausmekanismi ja LDAP-palvelimen nimi.



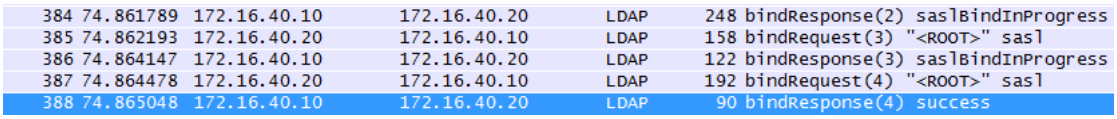
KUVIO 81. LDAP bindingRequest

AD-palvelin vastaa ACS-palvelimelle ”bindingRequest”-viesteillä, joiden tehtävänä on saada sovittua käytettävistä autentikaatiometodeista. Kun autentikointimetodeista on sovittu niin AD-palvelin lähettää viestin, jossa hyväksytään autentikaatiometodit. Kun LDAPissa käytettävistä salausmekanismeista on sovittu, tekee ACS-palvelin LDAP-haun joka on salattu. Kuviossa 82 on esitetty tapahtuma, jossa ACS-palvelin ehdottaa ”winkkarir2.labra.local”-hakemistopalvelimelle autentikaatioon käytettäväksi SASL-protokollaa jonka mekanismina toimii tarkemmin GSSAPI eli käyttäjät tunnistetaan käyttäen kerberos-protokollan versiota 5.



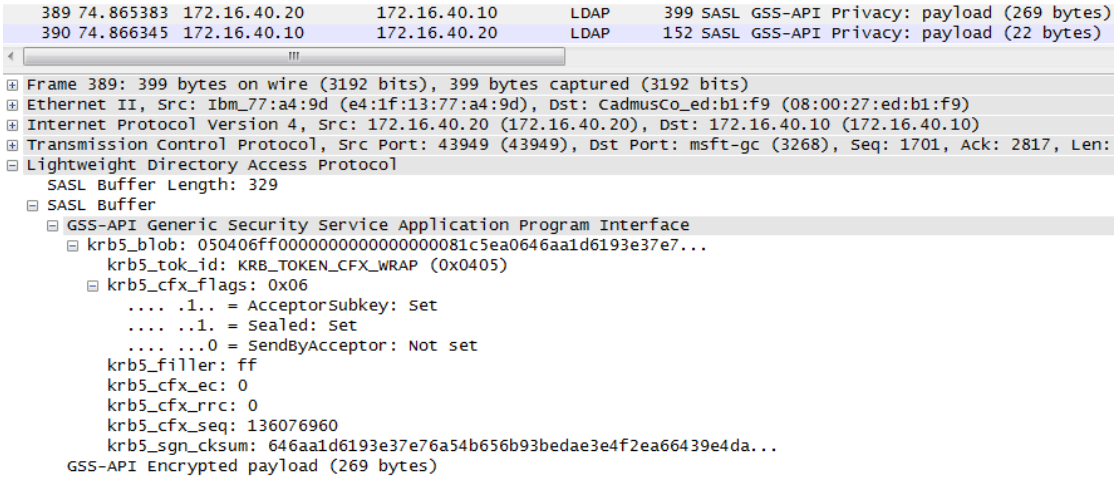
KUVIO 82. ACS–palvelimen lähettämä bindRequest-viesti

Seuraavaksi AD-palvelin lähettää ”bindResponse”-viestin jolla AD-palvelin ilmoittaa, että haluaa ACS-palvelimen lähettävän tälle uuden ”bindRequest”-viestin samalla SLAS-mekanismilla, jotta prosessia voidaan jatkaa. Kuviossa 83 on loput viestit, joissa sovitaan autentikaatiomenetelmistä, joka lopulta päättyy AD-palvelimelta tulleeseen ”bindResponse”-viestiin ”success”.



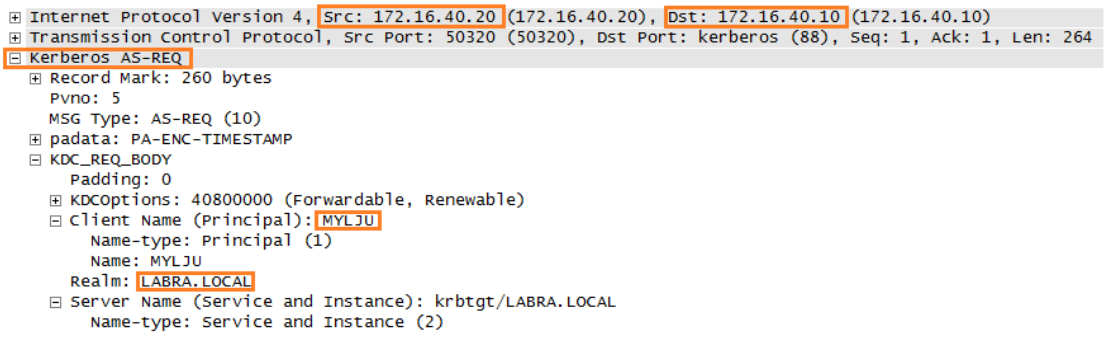
KUVIO 83. Autentikaatiometodeista sopiminen

Kun metodit on sovittu, kysyy ACS-palvelin AD-palvelimelta käyttäjätunnuksen sovituilla salausmetodeilla jotka ovat ”SASL GSS-API”. Kuviossa 84 on salattu LDAP-viesti, jolla ACS-palvelin hakee käyttäjän aktiivihakemistosta.



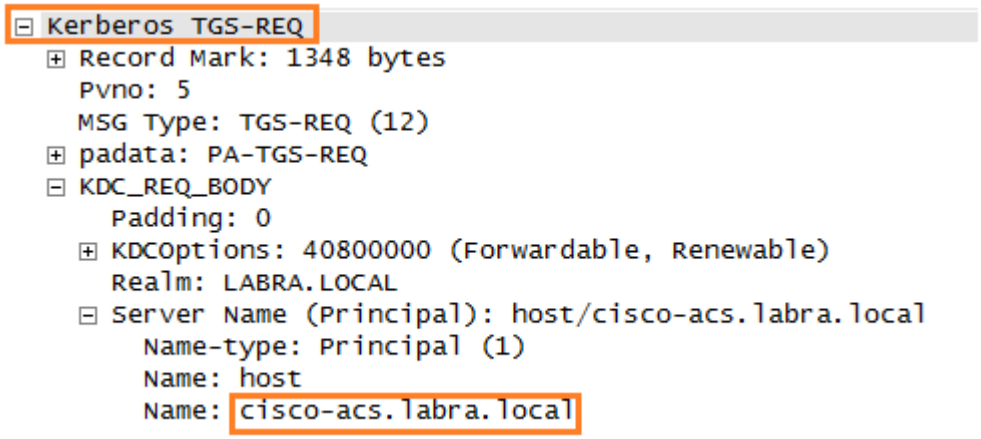
KUVIO 84. Suojattu LDAP-kysely

Kun käyttäjä on onnistuneesti haettu tietokannasta, aloitetaan tunnistaminen käyttäen kerberos-protokollaa. Ensimmäisenä ACS-palvelin lähettää AD-palvelimelle käyttäjätunnuksen ja toimialueen nimen. Kuviossa 85 on ACS-palvelimen lähettämä Kerberos-viesti.



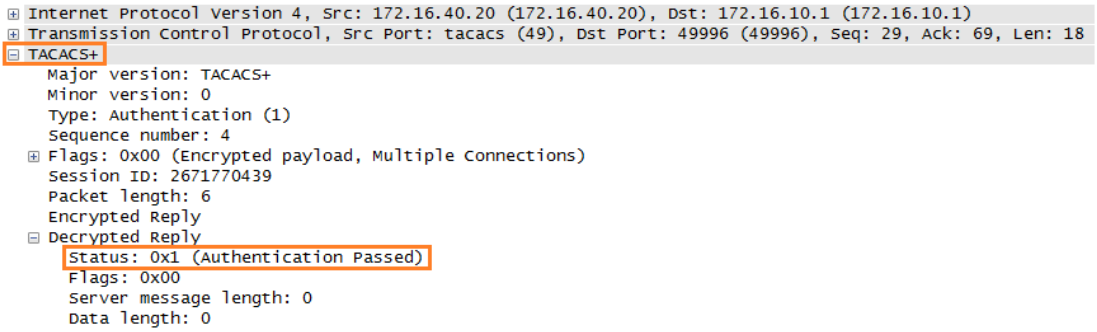
KUVIO 85. Käyttäjän tunnistaminen – ACS-palvelimen lähettämä Kerberos-viesti

Tähän viestiin AD-palvelin vastaa AS-REP-viestillä, jossa kerrotaan, että kyseinen käyttäjä löytyi kyseiseltä palvelimelta. Seuraavaksi ACS-palvelin tunnistautuu kerberos-viestillä ”TGS-REQ”, joka on esitelty kuviossa 86.



KUVIO 86. Kerberos TGS-REQ laitteen tunnistus

Tämän viestin AD-palvelin kuittaa TGS-REP-viestillä. Seuraavaksi hoidetaan loppuun käyttäjän tunnistetietojen välittäminen LDAP-protokollalla ja ACS-palvelin voi lähettää NAS-laitteelle viestin autentikaation onnistumisesta. Kuviossa 87 on TACACS+-viesti, jossa ilmoitetaan onnistuneesta autentikaatiosta.



KUVIO 87. Onnistunut autentikaatio

Kuviossa 88 on ACS-palvelimelta kaapattu *”access-policy”*-tieto, josta nähdään tarkemmin mitä politiikkaa autentikaatioon on käytetty.

Access Policy

Access Service:	Default Device Admin
Identity Store:	AD1
Selected Shell Profile:	Permit Access
Active Directory Domain:	labra.local
Identity Group:	
Access Service Selection Matched Rule :	AD-rule1
Identity Policy Matched Rule:	Default
Selected Identity Stores:	AD1, AD1
Query Identity Stores:	
Selected Query Identity Stores:	
Group Mapping Policy Matched Rule:	
Authorization Policy Matched Rule:	Default
Authorization Exception Policy Matched Rule:	

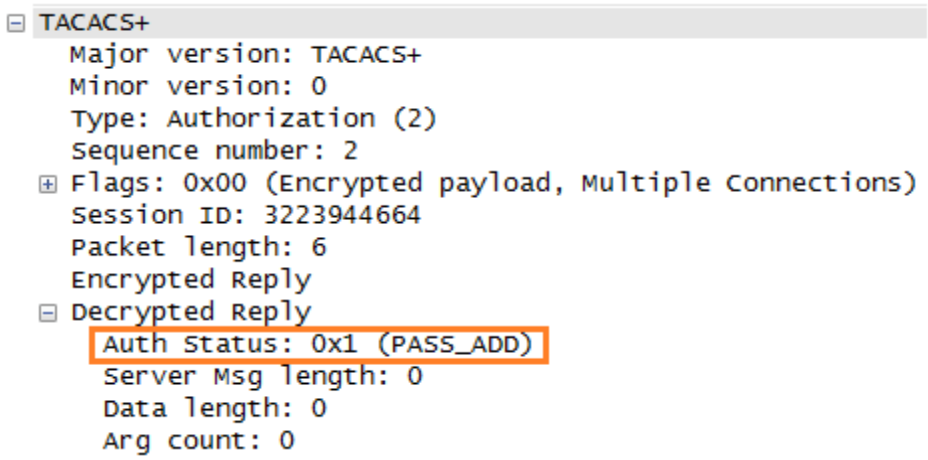
KUVIO 88. ACS-palvelimen Access Policy AD:ta vasten kirjautuessa

Käyttäjän tunnistuksen jälkeen valtuuttaminen tapahtuu täysin NAS-laitteen ja ACS-palvelimen välillä. Kuviossa 89 on valtuuttamispyyntö-viesti, jonka NAS-laite on lähettänyt ACS-palvelimelle.

```
⊟ TACACS+
    Major version: TACACS+
    Minor version: 0
    Type: Authorization (2)
    Sequence number: 1
  ⊞ Flags: 0x00 (Encrypted payload, Multiple Connections)
    Session ID: 3223944664
    Packet length: 50
    Encrypted Request
  ⊟ Decrypted Request
      Auth Method: TACACSPLUS
      Privilege Level: 1
      Authentication type: ASCII
      Service: Login
      User len: 5
      User: mylju
      Port len: 6
      Port: tty194
      Remaddr len: 12
      Remote Address: 172.16.40.10
      Arg count: 2
      Arg[0] length: 13
      Arg[0] value: service=shell
      Arg[1] length: 4
      Arg[1] value: cmd*
```

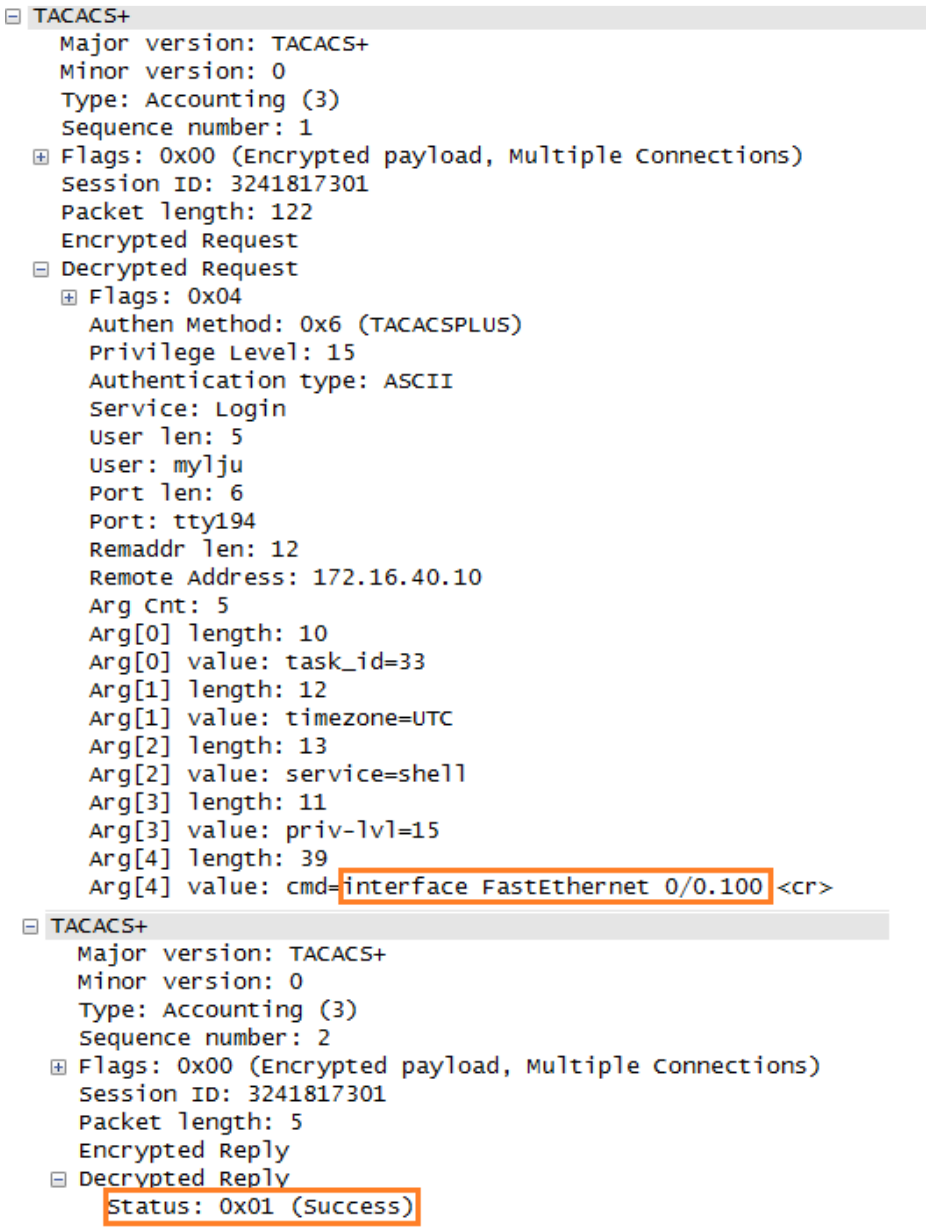
KUVIO 89. Authorization–paketti

Tähän ACS-palvelin vastaa joko myöntävästi tai kieltävästi. Kuviossa 90 on kuvakaappaus jossa ACS-palvelin on lähettänyt myöntävän vastauksen.



KUVIO 90. Authorization pass-viesti

Kirjanpito-osiossa NAS-laite lähettää tapahtumat ACS-laitteelle jotka tälle on määritelty lähetettäväksi. Kuviossa 91 on kirjanpidosta todennus (Lähetys ja kuittaus).



KUVIO 91. Kirjanpidon suorite ja kuittaus

Työssä ei nähty oleelliseksi dokumentoida kirjautumista erikseen kun ACS-palvelin käyttää paikallista käyttäjätietokantaa, sillä kyseinen tapahtuma on esitetty liitteessä 3 ja on toiminnaltaan täysin samanlainen kun käytettäessä ulkoista käyttäjätietokantaa lukuun ottamatta LDAP-kyselyä ja Kerberos-tunnistautumista.

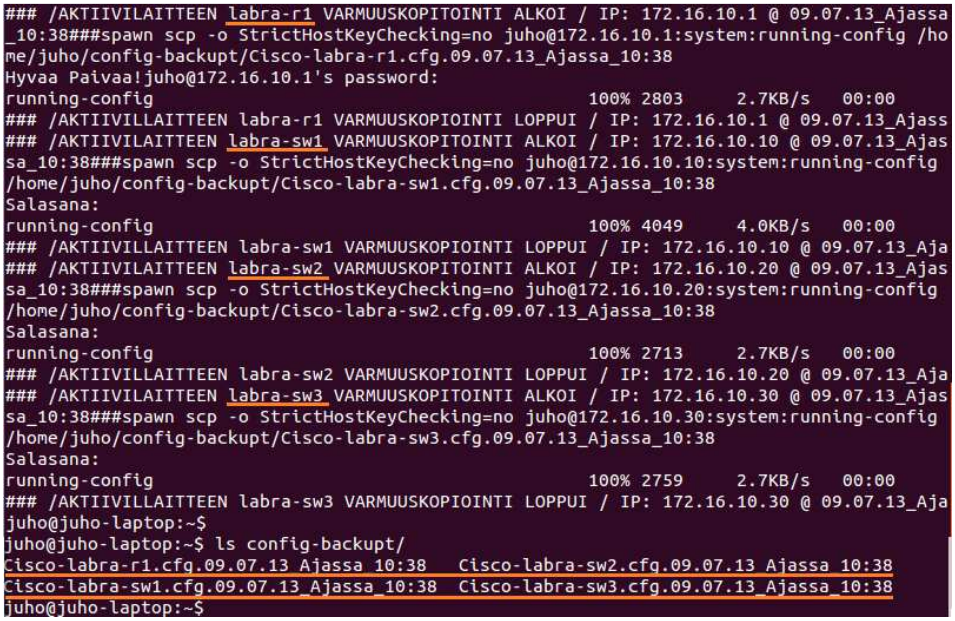
Autentikaatioprosessin toimivuus voidaan myös tarkistaa laitteelta käsin kuvion 92 mukaisesti.

```
Labra-sw2#test aaa group tacacs+ juho juho leg
Labra-sw2#test aaa group tacacs+ juho juho legacy
Attempting authentication test to server-group tacacs+ using tacacs+
User was successfully authenticated.

Labra-sw2#test aaa group tacacs+ juho juho1 le
Labra-sw2#test aaa group tacacs+ juho juho1 legacy
Attempting authentication test to server-group tacacs+ using tacacs+
User authentication request was rejected by server.

Labra-sw2#
```

KUVIO 92. Aktiivilaitteelta autentikaation testaaminen

Edellä olevassa kuviossa on suoritettu testi AAA ryhmälle *TACACS+* ja käyttäjälle *juho*. Kuviossa on myös haluttu näyttää se, että miltä näyttää tilanne jossa käyttäjätunnus salasanapari eivät täsmää TACACS+-palvelimella sijaitseviin tietoihin.

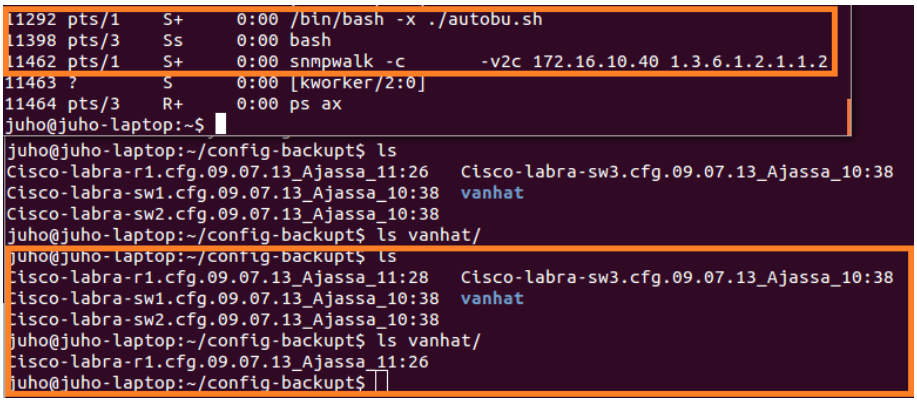
Konfiguraatioiden ja kirjautumisen jälkeen vuorossa oli laitteiden konfiguraatioiden varmuuskopiointi. Ensimmäisenä luotiin *.exp*-tiedosto, johon asetettiin *SCP*-komento hakemaan varmuuskopiot laitteiden nykyisistä konfiguraatioista. Ensimmäisenä testasin varmuuskopioinnin onnistumista ajamalla *.exp*-tiedoston samalta käyttöliittymältä kuin miltä konfiguraatiot suoritettiin. Kuviossa 93 on kuvankaappaus varmuuskopioinnin toiminnasta.



KUVIO 93. Käsin ajettu varmuuskopiointi Cisco Systems -laitteisiin

Edellä olevassa kuviossa on varmuuskopiointi skriptiin määritetyn loki-tiedoston sisältöä sekä lopussa on komento, jolla on listattu *”config-backupt”*-kansion sisältöä josta voidaan havaita, että konfiguraatioiden varmuuskopiot on tallennettu oikeaan paikkaan, aivan kuten skriptin piti tehdä.

Seuraavaksi todennettiin aikaisemmin esitetyn *Crontab*-toiminnon avulla ajastetun automaattisen varmuuskopioinnin toimintaa. Kuviossa 94 on esitetty tapahtuma, jossa Ubuntuun on syötetty *”ps ax”*-komento jolla on listattu prosessit sekä se, että konfiguraatiotiedostojen vertailu on onnistunut. *Labra-r1*-laitteeseen tehtiin muutos ennen ajastettua varmuuskopiointia jonka avulla todennus suoritettiin.



KUVIO 94. Ajastettu varmuuskopiointi ja konfiguraatioiden vertaus

Edellä olevasta kuviosta havaitaan, että *labra-r1*-laitteelle on tullut uusi konfiguraatiotiedosto ja vanha on siirretty kansioon *”vanhat”*, aivan kuten automaattisen varmuuskopioinnin piti tehdä. Muiden laitteiden konfiguraatiotiedostoja ei ole taltioitu, sillä ne eivät olleet muuttuneet. Vanhat konfiguraatiotiedostot on hyvä säästää, jotta tarvittaessa voidaan seurata konfiguraatiohistoriaa. Kuviosta on myös havaittavissa prosessien osalta se, että varmuuskopiointi pyörii vielä taustalla ja on tekemässä parhaillaan SNMP-kyselyä *labra-sw4*-laitteelle, joka oli Dellin laite ja näin ollen pystyttiin todentamaan Cisco-konfiguraatioiden avulla skriptin toiminnan.

Varmuuskopioinnin implementoituessa tuotantoympäristöön on syytä seurata sen toimintaa. Tähän on yksinkertainen tapa seurata raportointi-osiossa luotua web-sivustoa. Sivua katseltaessa viikoittain pitäisi kuviossa olla havaittavissa päivittäin suuri määrä onnistuneita autentikaatioita sillä jokainen varmuuskopiointi jättää autentikaatiojäljen. Mikäli epäonnistuneita autentikaatioita on todella paljon, on syytä ryhtyä tutkimaan onko varmuuskopiointi suoriutunut onnistuneesti. ACS-palvelin voidaan määrittää myös lähettämään sähköpostia tiettyjen raja-arvojen saavuttua, mutta tätä ei nähty tarpeelliseksi sillä ajastetut skriptit eivät suorita komentoja jotka voisivat aiheuttaa ongelmia verkkoon. Kyseinen sähköpostitoiminto olisi järkevämpi esimerkiksi 802.1x-asetusten kanssa, koska tällöin suuri määrä epäonnistuneita autentikaatioita voi viitata siihen, että suuri määrä koneita ei ole päässyt verkkoon. ACS-palvelin mahdollistaa myös raporttien viemisen ulos järjestelmästä, mutta tämä on tehtävä palvelimella erikseen käsin joka johtaa usein siihen, ettei myöhemmässä vaiheessa kyseistä toimintoa jakseta tehdä ja raportointi jää puolitiehen. Tästä syystä automaattinen raportointi web-sivustolle nähtiin tarpeelliseksi.

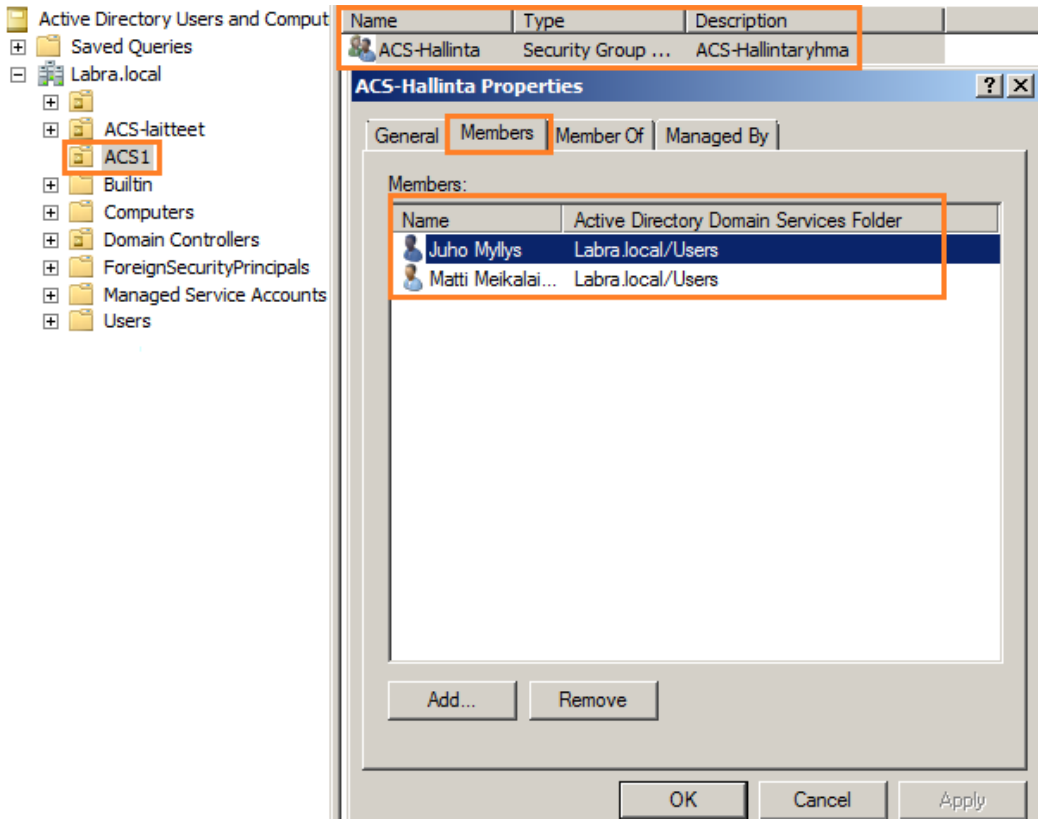
AD-palvelimen konfigurointi onnistui sulavasti käyttäen liitteen 15 Excel-tiedostoon luotuja komentoja. Ensimmäisenä ”maalattiin” Excel-tiedostosta halutut K-sarakkeen osat ja kopioitiin (copy) kyseiset tiedostot AD-palvelimen komentoriville (paste). Kuviossa 95 ja 96 on esitetty konfiguraation toimivuus.

```
C:\Users\Administrator>dsadd ou ou=ACS1,dc=Labra,dc=local
dsadd succeeded:ou=ACS1,dc=Labra,dc=local

C:\Users\Administrator>dsadd group cn=ACS-Hallinta,ou=ACS1,dc=Labra,dc=local -se
cgrp yes -desc ACS-Hallintaryhma
dsadd succeeded:cn=ACS-Hallinta,ou=ACS1,dc=Labra,dc=local

C:\Users\Administrator>dsmod group "cn=ACS-Hallinta,ou=ACS1,dc=Labra,dc=local" -
addmbr "cn=Juho Myllys,cn=Users,dc=Labra,dc=local"
dsmod succeeded:cn=ACS-Hallinta,ou=ACS1,dc=Labra,dc=local

C:\Users\Administrator>dsmod group "cn=ACS-Hallinta,ou=ACS1,dc=Labra,dc=local" -
addmbr "cn=Matti Meikalainen,cn=Users,dc=Labra,dc=local"
dsmod succeeded:cn=ACS-Hallinta,ou=ACS1,dc=Labra,dc=local

C:\Users\Administrator>dsmod group "cn=ACS-Hallinta,ou=ACS1,dc=Labra,dc=local" -
addmbr "cn=Teppo Testaaja,cn=Users,dc=Labra,dc=local"
dsmod failed:cn=ACS-Hallinta,ou=ACS1,dc=Labra,dc=local:Directory object not foun
d.
type dsmod /? for help.
C:\Users\Administrator>_
```

KUVIO 95. AD-palvelimen konfigurointi

Kuviota 95 tarkastellessa huomataan, että lopussa on yritetty lisätä käyttäjä jota AD-palvelimelta ei löydy. Tällaisesta ei varsinaisesti ole haittaa, sillä kyseinen toiminto näkyy ainoastaan herjana komentorivillä.

Kuviossa 96 on esitetty AD-palvelimelta graafisen näkymän avulla tapahtuma.



KUVIO 96. AD-palvelimen todennus

Kuviota 96 tarkastellessa huomataan, että AD-palvelimelle on konfiguroitunut OU nimeltä *”ACS1”***,** käyttäjäryhmä *”ACS-hallinta”*, joka on liitetty OU:hun *”ACS1”* ja ryhmään on liitetty kaksi jäsentä *Juho Myllys* ja *Matti Meikalainen*. Exceliä hyödyntäen saavutettiin todella nopea tapa konfiguroida AD-palvelimelle OU:ita, ryhmiä sekä liittää näihin käyttäjiä.

7.1 AAA ja VAHTI

Taulukossa 10 on esitetty AAA-arkkitehtuurin eri osa-alueet laitevalmistajakohtaisesti.

TAULUKKO 10. AAA osa-alueet laitevalmistajakohtaisesti

	Cisco	Dell	HP
Tunnistus	X	X	(X)
Valtuuttaminen	X		(X)
Kirjanpito	X		(X)

Taulukkoa 10 tarkastellessa huomaamme, että Cisco Systemsin laitteet mahdollistivat jokaisen osa-alueen AAA-arkkitehtuurista. Dellin laite vastaavasti ei mahdollistanut muuta kuin tunnistautumisen TACACS+-palvelinta vasten. HP:n laitetta laboratorioympäristössä ei ollut käytettävissä mutta komentoja ja manuaalia selaamalla, on tuloksena kuitenkin se, että HP mahdollistaa jokaisen AAA-arkkitehtuurin osa-alueen.

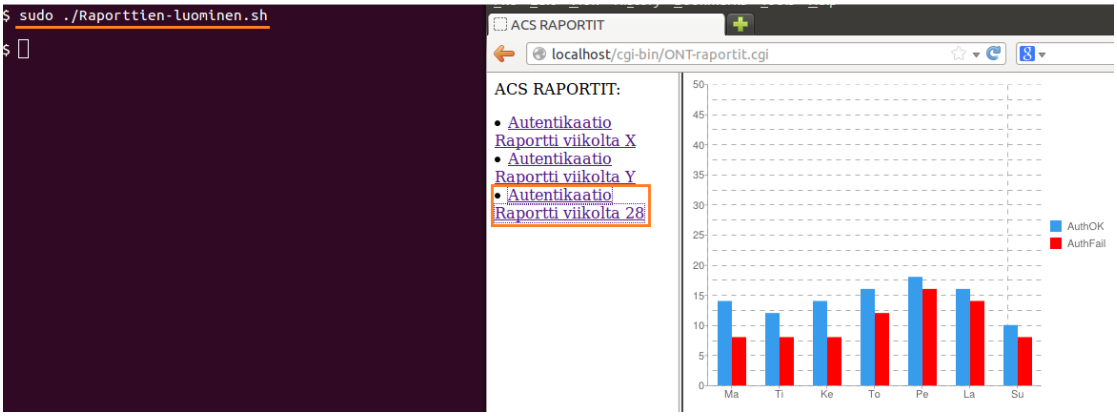
Tästä osiosta voidaan jo päätellä, että laboratorioympäristössä ollut Dellin valmistama laite ei täytä VAHTI-ohjeen osa-alueita niin hyvin kuin kaksi muuta laitevalmistajaa. Koska kirjanpito-osio ei onnistu lainkaan, ei voida Dellin laitteistolle suoritettuja komentoja kirjata ja näin ollen *”audit trail”* ei onnistu. HP:n laitteiden pääsylistat eivät olleet niin kattavia kuin Dellin tai Cisco Systemsin laitteiden kohdalla. HP:n laitteiden pääsylistoille sallitaan minkä tahansa protokollan liikennöinti mutta vain tietyistä IP-osoitteista, kun taas Cisco ja Dell laitteissa pystyttiin rajaamaan myös turhat protokollat pois.

Yleisesti eri VAHTI osa-alueet esiteltiin niiden konfiguroinnin yhteydessä ja pääasiassa jokainen osa-alue saatiin hoidettua ympäristöön nähden parhaalla mahdollisella

tavalla. Liitteeseen 17 on listattu eri osa-alueet ja niiden ratkaisut sekä se, että tuliko kyseinen VAHTI sisäverkko-ohjeen osa suoritettua vai ei.

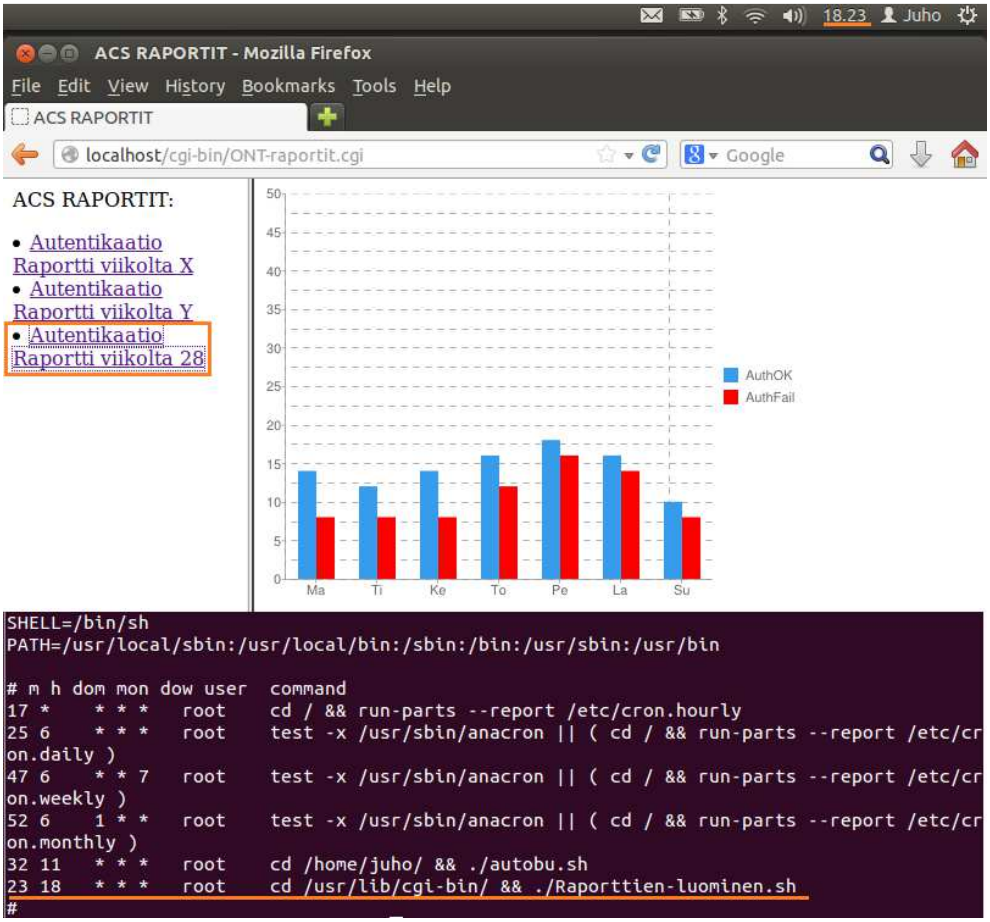
7.2 Raportointi

Raportoinnin idea oli, kuten aikaisemmin esitettiin, että kaaviot lisääntyisivät automaattisesti jotta raporttien seuraaminen olisi mahdollisimman yksinkertaista. Ensiksi todensin kyseisen ominaisuuden ajamalla skriptin käsin ja varmentamalla, että linkki lisääntyy web-sivustolle oikein. Kuviossa 97 on esitelty skriptin manuaalinen ajo sekä se, että sivustolle on lisääntynyt uusi linkki.



KUVIO 97. Linkin lisäys skriptillä

Seuraavaa testiä varten jouduin poistamaan ensiksi manuaalisesti kyseisen linkin tiedostosta *”Raportit.cgi”* josta tiedosto *”ONT-raportit.cgi”* lukee linkit. Tämän jälkeen ajastin *crontab* ominaisuudella skriptin ja kuviossa 98 on todennettu, että automaattinen linkin lisääminen onnistui.



KUVIO 98. Ajastettu linkin lisäys

Kuten edellä olevasta kuviosta voidaan havaita, on sama linkki (Vko 28) lisääntynyt nyt automaattisesti *crontab*-toiminnon avulla.

8 YHTEENVETO

8.1 Tuloksien yhteenveto

Työ alkoi tutustumisella RADIUS ja TACACS+-protokolliin sekä AAA-arkkitehtuuriin yleisesti. Alussa tuntui, että työ on melko suppea. Työn edetessä alkoi työmäärä lisääntyä, sillä halu kehittää tapaa, jolla kyseiset toiminteet voidaan toteuttaa verkkoon, oli suuri. Konfiguraatioita oli loppujen lopuksi paljon ja työn suunnitteluosuus osoittautui hieman haasteelliseksi, sillä palvelimien ja niiden palveluiden käyttö oli melko vierasta minulle työn alkuvaiheessa. Suunnittelu on muutenkin kattava kokonaisuus, mikäli sen haluaa tehdä hyvin. Suunnittelu sisältää usein protokollan valinnasta toteutukseen kaiken oleellisen kuten konfiguraatioiden ajamisen laitteisiin sekä toimintojen todentamisen.

Skriptien ohjelmoiminen oli minulle työn alussa melko vierasta mutta halusin hieman kuluttaa tähän aikaani, sillä kyseinen taito on nykypäivänä tietoliikenteen alalla todella hyödyllinen.

Aikaisempaa kokemusta aiheesta oli sen verran, että olin konfiguroinut aikaisemmin Cisco Systemsin laitteille tunnistautumisen RADIUS-protokollaa käyttäen Linux-palvelimessa pyörivää FreeRADIUS-ohjelmistoa vasten.

Opinnäytteen tuloksena rakentui keskitetty käyttäjähallinta aktiivilaitteille. Toiminto oli toimiva käytettäessä ulkoista tai sisäistä käyttäjätietokantaa. AAA-arkkitehtuurin jokainen osa-alue saatiin onnistuneesti todennettua WireShark-ohjelmiston avulla. AD-palvelimen ja ACS-palvelimen integroiminen sekä käyttäjien hakeminen aktiivihakemistosta onnistui hyvin. Aktiivilaitteiden konfigurointi onnistui todella vaivattomasti skriptin rakentamisen jälkeen. Neljän verkkolaitteen AAA ja SSH-konfiguraatioihin meni aikaa ainoastaan 21 sekuntia, joka todennettiin käyttäen WireShark työkalua, kuten aikaisemmin esitettiin.

Automaattinen varmuuskopiointi verkkolaitteilta ei ollut tietoturvallisin tapa, mutta ilman maksullista erillistä ohjelmaa, mielestäni kuitenkin fiksuin ja ehdottomasti halvin keino.

Työ ei ollut luonteeltaan protokollien tutkimista ja niiden todentamista mutta kiinnostus aiheeseen kasvoi, mitä enemmän työssä etenin. Näin ollen data-liikennettä tutkiessani huomasin, että TACACS+-protokolla toimii pääosin TACACS+-dokumentin kuvaamalla tavalla. RADIUS-protokollaa tutkin myös käytännön kautta joka mahdollisti sen, että pystyin todentamaan RADIUS-protokollan vastaavuuden RFC-dokumenttiin. WireShark-työkalu onneksi mahdollisti salaisenavaimen syöttämisen avulla avaamaan TACACS+-paketteja, jotta protokollan eri toimintatavat olivat näkyvillä ja niitä pääsi tutkimaan.

VAHTI osa-alueet toteutettiin verkkoon melko kattavasti siihen nähden kuinka pieni ympäristö minulla oli käytössä. VAHTI ohjetta noudattaessa oli huomioitavaa sellainen seikka, että erilaiset ihmiset omaavat erilaisia näkemyksiä siitä miten jokin viite tulisi luoda ja mikä on pohjimmiltaan viitteen tarkoitus. Opinnäytetyössä en lähtenyt salasanapolitiikkaa sen pidemmälle viemään, kuin mitä hieman ACS-palvelimelle kirjautuessa esitin. Tuotantoympäristössä on kuitenkin tärkeää, että salasanapolitiikka on säädetty jokaiseen verkon osioon suhteellisen hankalaksi mutta kuitenkin sellaiseksi, että käyttäjien hermot säilyvät eli käytettävyys pysyy asiallisena. Mielenkiintoista olisikin nähdä, että mikäli AD-palvelimelle asetetaan salasanapolitiikan osaksi se, että käyttäjien tulee vaihtaa salasanaa tietyin väliajoin niin tajuaako ACS-palvelin heti kyseisen muutoksen vai pääseekö verkkolaitteille kirjautumaan edelleen vanhalla salasanalla. Mikäli ACS-palvelin liitetään AD-palvelimeen, on syytä miettiä halutaanko käyttää rahaa suuria määriä itse palvelimeen sillä kyseinen palvelin toimii ikään kuin TACACS+-välityspalvelimena eli siihen nähden melko kallis hankinta. Vaihtoehtoisesti kyseisen toiminteen voisi hankkia palveluna. Vaikka opinnäytetyön pääpainoarvona ei ollut tietoturvan kehittäminen ja suunnittelu tuli hyvin äkkiä VAHTIn kautta selväksi se, että käytettävyyden pitäminen tasapainossa mahdollisemman korkean tietoturvallisuuden kanssa vaatii kovaa työtä jo pienessä mittakaavassa.

Työstä tuli melko pitkä, sillä halu tutkia protokollien toimintaa ja halu todentaa niiden toiminta mahdollisimman tarkasti osoittautui työlääksi mutta opettavaiseksi. Myös halu kehittää konfiguraatioiden suorittamista verkkolaitteisiin kasvoi mitä enemmän työssä etenin. Tietoliikenteen seuraaminen ja datan analysointi on todella opettavaista ja voin suositella sitä ihan arkielämässä kuten WWW-sivujen selaamisen yhteydessä.

Kokonaisuutta miettiessä olen erittäin tyytyväinen tuotokseen, sillä laboratorioympäristön vaatimattomuuteen nähden sain aikaiseksi todella hyvän järjestelmän ja toimivat konfiguraatiot niin tiedonvälityslaitteille kuin palvelimille. Opinnäytteen nimen sisältäessä *”Suunnittelu ja toteutus”* oli otettava huomioon paljon muitakin asioita kuin ainoastaan se, että saan toteutettua toimivan autentikaation keskitettyä käyttäjätietokantaa vasten vaan oli myös huomioitava erilaisia seikkoja kuten konfiguraatioiden suorittaminen. Mikäli aloittaisin työn tekemisen nyt, niin ehdottomasti käyttäisin aluksi aikaa enemmän myös palvelimien manuaalien lukemiseen enkä intoa täynnä itse opettelisi niiden käyttöä.

Opinnäytetyössä törmäsin muutamiin ongelmiin, joihin pääasiassa löysin vastaukset.

HTML-kieli oli uutta eli en ollut koskaan aikaisemmin käyttänyt kyseistä kieltä. Koodia tuli kuitenkin niin vähän, että HTML koodin opiskelu ei tuottanut päänvaivaa ja koulussa oli aikaisempaa kokemusta pienestä *PHP*:n käytöstä.

Bash skripteistä ei ollut aikaisempaa kokemusta mutta koulussa olin opiskellut yhden erikoistumismoduulin yhteydessä hieman *python*-kielen perusteita, josta oli nyt hyötyä rakenteita miettiessä ja muuttujia käyttäessä.

Varmuuskopioinnin automatisointi tuotti ongelmia alusta alkaen. Varmuuskopiointiin yritin suunnitella mahdollisimman tietoturvallisen keinon, joka on jossain määrin käyttäjäystävällinen sekä luotettava. Tästä syystä työssä käytettiin *”Backuppaaja”*-nimistä käyttäjää, jolle oli syötetty pitkä ja todella monimutkainen salasana ja kyseisen käyttäjätunnuksen kirjautumisaikaa rajoitettiin ainoastaan kellon aikaan, jolloin varmuuskopiointi on sallittua. Tiedosto jossa käyttäjätiedot sijaitsivat suojattiin tavalla joka mahdollisti sen, että kuka tahansa ei pääse katsomaan tiedoston sisältöä.

Edellä mainittu asia kuitenkin aiheutti sen, että mikäli käyttöliittymän kautta suoritetaan varmuuskopiointi, niin tulee se suorittaa *”sudo”*-komennolla, joka puolestaan taas laskee hieman käytettävyyden tasoa.

Työn liitteiksi en liittänyt kuin Cisco Systemsin laitteisiin liittyvät konfiguraatio ja varmuuskopiointi-tiedostot, sillä työn pituus olisi kasvanut entisestään ja kyseiset tiedostot ovat hyvin pitkälti identtisiä keskenään, ainoastaan komentojen syntaksi muuttuu hieman. Opinnäytetyöhön varatut 15 opintopistettä riittivät melko hyvin ajallisesti, kun ajan käytti alusta asti tehokkaasti ja suunnitteli työn tekemisen etukäteen mahdollisimman pitkälle.

8.2 Vaikutus tietoturvaan

Opinnäytetyöllä oli vaikutusta tietoturvaan, sillä hallinta yhteydet saatiin vaihdettua suojaamattomasta telnet:stä SSH-protokollaan, varmuuskopiointtiin käytettiin suojattua SCP-protokollaa ja geneerisestä käyttäjätunnuksesta päästiin teoriassa eroon. Laitteisiin on syytä jättää geneeriset tunnukset joita käyttäen päästään hallitsemaan kytkimiä vikatilanteissa konsoli-linjaa pitkin. Tämä ei heikennä tietoturvaa sillä kytkimet ovat fyysisesti suojatuissa konesaleissa, joihin ei ole pääsyä kuin valtuutetuilla henkilöillä näin ollen konsoli-linjaan ei pääse ulkopuoliset henkilöt käsiksi. HP:n tuotteessa käyttöön valittiin *Secure Backdoor*-toiminne, joka mahdollistaa siis sisäisellä tunnuksella kirjautumisen, mikäli TACACS+-palvelin ei ole tavoitettavissa. Näin ollen teoriassa HP:n laitteisiin ei pääse käsiksi geneerisellä tunnuksella. VAHTI-ohjeen kohdat nostattivat myös tietoturvan tasoa, sillä verkkoon saatiin uusia käytänteitä kuten ’*Audit trail’*-toiminto, jonka kautta pystytään seuraamaan verkkoon luotuja tapahtumia. Lyhyesti voidaan todeta, että VAHTI-ohjeen avulla saatiin verkkoon melko paljon lisättyä tietoturvaa.

8.3 Tulevaisuuden pohdinta

Ensimmäinen opinnäytetyöni jatkokehityskohde tulevaisuudessa olisi ehdottomasti ACS-palvelimen kahdennus tai kasata isompi klusteri, jotta TACACS+-prosessit eivät pysähtyisi yhden palvelimen kaatumiseen. ACS-palvelimen näkyvyyttä voisi myös parantaa jotta päästäisiin mahdollisesti eroon siitä, että lokeja pitäisi tutkia palvelimen kautta tekstimuodossa, kuten opinnäytteessä tehtiin autentikaatioille. Raportointi osiota on syytä jalostaa hieman ennen kuin se viedään tuotantoympäristöön. On syytä miettiä, minkälaisia asioita halutaan kerätä web-sivustolle ACS-lokeista. Googlen palvelun käyttö on harkinnan varaista ja aina on suotavampaa, että käytettäisi itse tehtyä graafia, jotta hallinta-aseman ei tarvitsisi olla missään yhteydessä julkiseen verkkoon. Opinnäytetyössä käytettiin Googlen palvelua, jotta työurakka hieman helpottui.

Mikäli jokainen verkkolaite mahdollistaa tulevaisuudessa Linux-palvelimen tapaan avaimeen perustuvan kirjautumisen, on syytä muuttaa varmuuskopiointiin käytettävän tunnuksen salasana avaimeen ja luoda mahdollisesti kyseinen tunnus itse verkkolaitteisiin, mikä lisää varmuuskopioinnin tietoturvaa.

Skriptiä olisi hyvä hyödyntää jatkossakin ja laajentaa sen toimintaa. Verkkojen kanssa työskentelevät voisivat pohtia mitkä osa-alueet ovat verkossa sellaisia, joita joudutaan muuttamaan paljon, esimerkiksi VLANin lisäys trunk-linkille tai IP-osoitteen lisääminen ACL:ään. Varmuuskopiointiin olisi hyvä kehittää osa-alue, joka pakkaa kaikki vanhat laitteiden konfiguraatiot yhdeksi tiedostoksi, kun niitä on esimerkiksi 50 kpl.

LÄHTEET

Bhaiji, Y. 2008. Network Security Techonologies and Solutions (CCIE Professional development Series) ISBN:9781587052460

Carrel, D. & Grant, Lol. 1998 Draft-grant-tacacs-00.txt. Cisco Systems

Cisco Systems ACS 5.x and later integration with Microsoft Active Directory Configuration. Viitattu 20.6.2013 Http://www.cisco.com/en/US/products/ps9911/products_configuration_example09186a0080bc6506.shtml

Cisco Systems Catalyst 2960 Switch Software Configuration Guide 2009

Dell PowerConnect PCM6220, PCM6348, PCM8024, PCM8024-k CLI Reference Guide 2011

Dwivedi, H. 2004 Implementing SSH: Strategies for Optimizing the Secure Shell ISBN:9780471458807

Hewlett Packard. 2013 HP IMC Specifications viitattu 22.5.2013 http://www8.hp.com/uk/en/products/network-management/product-detail.html?oid=5032113#!tab=specs

HP GbE2c Ethernet Blade Switch for c-Class BladeSystem Command Reference Guide 2006

Linux dialog utility tutorial. 2013 Unix Command Line viitattu 25.7.2013 http://www.unixcl.com/2009/12/linux-dialog-utility-short-tutorial.html

Miten SSH toimii. 2013 Lintula viitattu 20.5.2013 http://www.cs.tut.fi/lintula/ software/ssh/teoria.shtml

Rigney Livinstong, C. 2000 RFC2866 RADIUS Accounting. Internet RFC Archives

Rigney, C., Rubens Merit, A., Simpson Daydreamer, W. & Willens Livingston, S. 2000 RFC2865 Remote Authentication Dial In User Service (RADIUS). Internet RFC Archives

Santuka, V., Banga, P & Carrol Brandon, J. 2011 AAA Identity Management Security. Pearson Education. ISBN:9781587141447

Tietoturvallisuus. 2013 Valtionvarainministeriö viitattu 4.6.2013 http://www.vm.fi/vm/fi/16_ict_toiminta/009_Tietoturvallisuus/index.jsp

Toiminta. 2013. Kansaneläkelaitoksen verkkosivut. Viitattu 15.5.2013 http://www.kela.fi/toiminta

Työjärjestys. 2013 Kansaneläkelaitoksen verkkosivut. Viitattu 15.52013 http://www.kela.fi/kansanelakelaitoksen-tyojarjestys

VAHTI tiivistelmä. 2013 Valtionvarainministeriö viitattu 4.6.2013 http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20101203Sisaeve/name.jsp

Valtionhallinnon tietoturvallisuus. 2013 Valtionvarainministeriö Sisäverkko-ohje viitattu 6.6.2013 http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20101203Sisaeve/Sisaeverkko-ohje.pdf

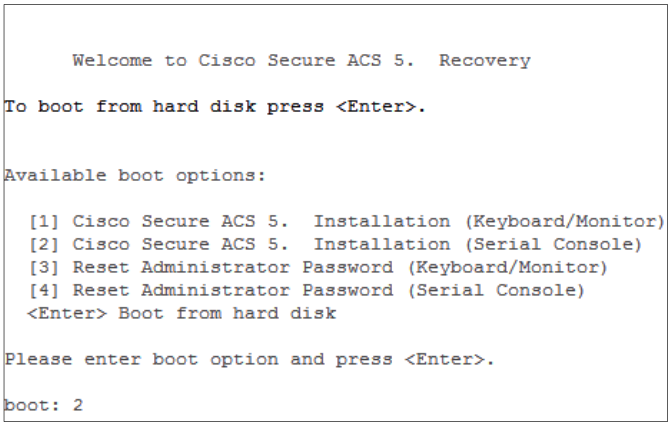
LIITTEET

Liite 1. RADIUS attribuutit

#	Attribute	Request	Accept	Reject	Challenge
1	User-Name	0 - 1	0 - 1	0	0
2	User-Password	0 - 1	0	0	0
3	CHAP-Password	0 - 1	0	0	0
4	NAS-IP-Address	0 - 1	0	0	0
5	NAS-Port	0 - 1	0	0	0
6	Service-Type	0 - 1	0 - 1	0	0
7	Framed-Protocol	0 - 1	0 - 1	0	0
8	Framed-IP-Address	0 - 1	0 - 1	0	0
9	Framed-IP-Netmask	0 - 1	0 - 1	0	0
10	Framed-Routing	0	0 - 1	0	0
11	Filter-ID	0	0+	0	0
12	Framed-MTU	0 - 1	0 - 1	0	0
13	Framed-Comperssion	0+	0+	0	0
14	Login-IP-Host	0+	0+	0	0
15	Login-Service	0	0 - 1	0	0
16	Login-TCP-Port	0	0 - 1	0	0
18	Reply-Message	0	0+	0+	0+
19	Callback-Number	0 - 1	0 - 1	0	0
20	Callback-ID	0	0 - 1	0	0
22	Framed-Route	0	0 - 1	0	0
23	Framed-IPX-Network	0	0 - 1	0	0
24	State	0 - 1	0 - 1	0	0 - 1
25	Class	0	0+	0	0
26	Vendor-Specific	0+	0+	0	0+
27	Session-Timeout	0	0 - 1	0	0 - 1
28	Idle-Timeout	0	0 - 1	0	0 - 1
29	Termination-Action	0	0 - 1	0	0
30	Called-Station-Id	0 - 1	0	0	0
31	Calling-station-Id	0 - 1	0	0	0
32	NAS-identifier	0 - 1	0	0	0
33	Proxy-State	0+	0+	0+	0+
34	Login-LAT-Service	0 - 1	0 - 1	0	0
35	Login-LAT-Node	0 - 1	0 - 1	0	0
36	Login-LAT-Group	0 - 1	0 - 1	0	0
37	Framed-AppleTalk-Link	0	0 - 1	0	0
38	Framed-AppleTalk-Network	0	0+	0	0
39	Framed-AppleTalk-Zone	0	0 - 1	0	0
40 - 59	Reserved for accounting				
60	CHAP-Challenge	0 - 1	0	0	0
61	NAS-Port-Type	0 - 1	0	0	0
62	Port-Limit	0 - 1	0 - 1	0	0
63	Login-LAT-port	0 - 1	0 - 1	0	0

Liite 2. ACS-palvelimen asennus

Ensimmäisenä ACS:n asennuksessa valittiin toimenpide, joka haluttiin laitteelle suorittaa. Valittiin kaksi (2) eli asennus sarjakonsolia käyttäen. Seuraavassa kuviossa on esitelty alkuvalikko.



ACS-asennus vaihe 1

Asennuksen jälkeen laite uudelleenkäynnistyy automaattisesti. Alla olevassa kuviossa on esitetty alkuasennuksen loppuminen

ACS-asennus vaihe 2

Ennen varsinaisia asetuksia laite pyytää siirtymään valikkoon, jotta voidaan aloittaa laitteen konfigurointi. Seuraavassa kuviossa on esitelty kyseinen tapahtuma.

```
**********************************************
Please type 'setup' to configure the appliance
**********************************************
localhost.localdomain login: setup
```

ACS-asennus siirtyminen konfiguraatio tilaan

Seuraavaksi laitteeseen asetetaan perusparametrit kuten isäntänimi, IP-osoite, verkkomaski, oletusyhdyskäytävä, DNS-toimialue ja ensisijainen DNS-palvelin. Seuraavassa kuviossa on esitelty oletusparametrien määrittäminen.

```
Press 'Ctrl-C' to abort setup
Enter hostname[]: cisco-acs
Enter IP address[]: 172.16.40.20
Enter IP netmask[]: 255.255.255.0
Enter IP default gateway[]: 172.16.40.1
Enter default DNS domain[]: labra
Enter primary nameserver[]: 172.16.40.10
```

Perusparametrit osa 1

Seuraavassa kuviossa on esitelty oletusparametrien toisen osan syöttäminen, missä laite kysyy, että halutaanko syöttää toinen nimipalvelin ja asetetaan aikavyöhyke. Laite pyytää myös salasanan. Seuraavassa kuviossa on esitelty mitä salasanat eivät saa sisältää.

```
Add secondary nameserver? Y/N : n
Enter primary NTP server[time.nist.gov]:
Add secondary NTP server? Y/N : n
Enter system timezone[UTC]: UTC+2
% Invalid time zone, please refer to your installation guide for list of timezon
es.
Enter system timezone[UTC]:
Enter username[admin]: admin
Enter password:
Enter password again:
Error: password must have at least six characters
Enter password:
Enter password again:
Error: password must have at least one upper case letter
Enter password:
Enter password again:
Error: password cannot contain "CcIiSsCcOo"
Enter password:
Enter password again:
Bringing up network interface...
```

Perusparametrit osa 2

Lopuksi laite käynnistyy ja siirrytään Ciscon laitteiden CLItä muistuttavaan tilaan. Alla on esitetty ’*show version*’-komento. Tarkempi ohjelmistoversio on poistettu näkyvistä.

```
cisco-acs login: admin
Password:
cisco-acs/admin# sh version

Cisco Application Deployment Engine OS Release: 2.
ADE-OS Build Version: 2.
ADE-OS System Architecture:

Copyright (c) 2005-2011 by Cisco Systems, Inc.
All rights reserved.
Hostname: cisco-acs


Version information of installed applications
---------------------------------------------


Cisco ACS VERSION INFORMATION
-----------------------------
Version : 5.
Internal Build ID : B.

cisco-acs/admin#
```

ACS-asennus valmis

Nyt laite on valmis käytettäväksi. Normaalitilanteessa laitteeseen otetaan selaimella yhteys IP-osoitteeseen, joka laitteelle määriteltiin esiasennusvaiheessa, käyttäen HTTPS-protokollaa.

Liite 3. Toimeksiantajalle ohje ACS-palvelimen konfiguroinnista

Huomioitavaa on, että ohjeessa esitetyissä kuvioissa on painettu ensiksi joko ”create” tai ”*add*”-näppäintä ja jokaisen tehdyn muutoksen jälkeen valitaan sivuston alareunasta joko ”*Submit*” tai ”*Save changes*” jotta tehdyt muutokset tulevat voimaan.

ACS-palvelimelle otetaan yhteys esiasennuksen yhteydessä määritettyyn IP-osoitteeseen käyttäen HTTPS-protokollaa. (esimerkki https://172.16.40.20, vaihtoehtoisesti voidaan käyttää nimipalveluun lisättyä nimeä https://IP:tä-vastaavanimi) Palvelimelle kirjaudutaan ensimmäistä kertaa *ACSadmin* tunnuksella, jolle vaihdetaan salasana.

Perusasetukset löytyvät kaikki oletussivun vasemmasta laidasta löytyvästä palkista, lopussa oleva monitorointi avautuu erilliselle sivulle. Kuvioita tarkastellessa huomataan, että lähes jokaisessa kuviossa on vielä erikseen näkyvissä polku asetusten asettamiseen, sekä kuvioihin on asetettu oranssilla värillä rajat, joita klikkailemalla päästään kyseiseen valikkoon. Esimerkkinä polusta on alla olevan kuvion mukainen rivi *”Network Resources > Network Device Groups > Location > create”*.

ACS-palvelimen konfigurointi on hyvä aloittaa siitä, että määritetään ensimmäisenä laitteille sijainnit. Ensimmäisenä luodaan tieto siitä, että kaikki laitteet sijaitsevat *Suomessa*.

Laitteiden maantieteellinen sijainti

Mikäli yrityksellä on useampia toimipisteitä joissa laitteita mahdollisesti sijaitsee, on sijaintia hyvä vielä tarkentaa. Seuraavassa kuviossa on luotu sijainti *”Labra”,* joka on sijoitettu suomen alueelle.

Sijainnin täsmentäminen

Laitteille voidaan edelleen määrittää tarkempia sijainteja. Laitteiden sijainnin tarkentamiseen on kuitenkin hyvä vetää raja johonkin, jotta myöhemmin itse laitteiden lisääminen ei käy liian työlääksi ja laitteet lisätään vain ryhmään *”All Locations”*. ACS-palvelimelta voidaan sijainti määrittelyjen jälkeen katsoa hierarkkisesta puusta mistä löytyy sijaintitiedot aina viimeiseen ”lehteen” saakka. Alla olevassa kuviossa on esitetty hierarkkinen näkymä laitteiden sijainnista.

Hierarkkinen näkymä laitteiden sijainnista.

Jotta laitteiden sijainnista olisi jotain hyötyä, on syytä luoda laitteille myös ryhmät. Ryhmittely on syytä miettiä valmiiksi ja mahdollisimman loogisella tavalla. Laitteet voidaan lajitella esimerkiksi valmistajan mukaan, toiminnallisuuden (L2 vs. L3) mukaan tai minkä tahansa muun asian mukaisesti. Seuraavaksi luodaan laiteryhmä ni-

meltä *kytkimet*. Koska kyseessä on ryhmä jonka alle tullaan sijoittamaan muita ryhmiä ja sille ei ole sopivaa esiryhmää, ei sille tällaista erikseen määritellä.

Laiteryhmän luominen

Laiteryhmille voidaan luoda täsmentäviä ryhmiä, aivan kuten laitteiden sijainnin tapauksessa. Seuraavassa kuviossa on luotu erilaisia laiteryhmiä, joissa on eroteltu mm. Kytkimien toimintataso (L2 & L3) sekä luotu laitevalmistaja kohtaisia ryhmiä.

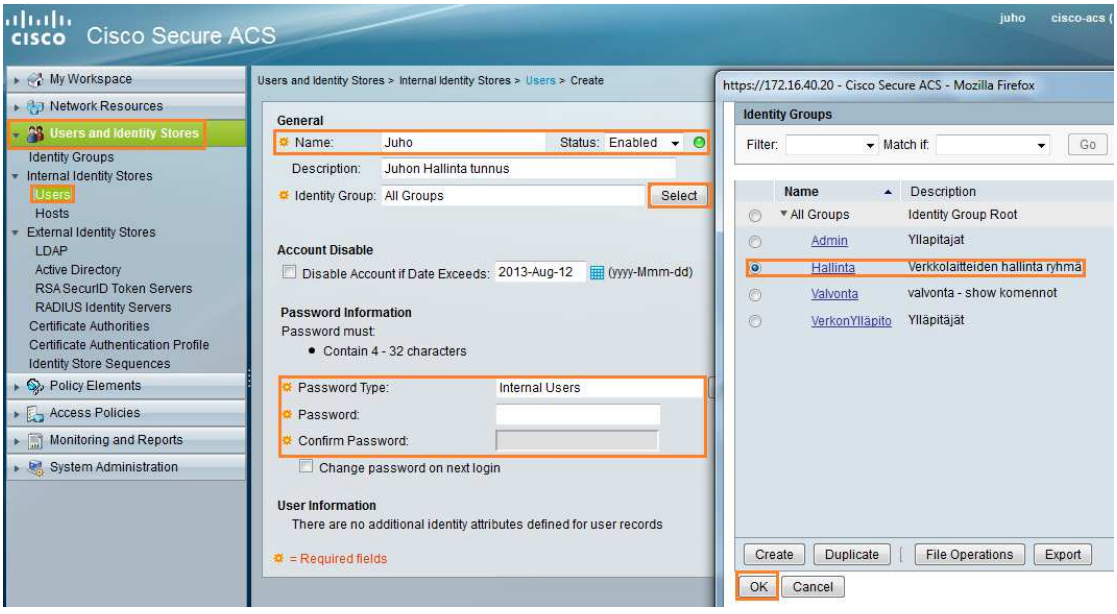
Laiteryhmien hierarkkinen näkymä

Kun edelliset ryhmät on luotu, voidaan aloittaa käyttäjäryhmien luominen. Käyttäjäryhmät on hyvä nimetä kuvaavasti, sekä niille kannattaa antaa kuvaus, josta voidaan päätellä ryhmän toimintataso. Seuraavassa kuviossa luodaan ryhmä nimeltä ”Valvonta”, jolle annetaan kuvaukseksi ”Verkkolaitteiden Valvonta ryhmä”.

Käyttäjäryhmän luominen

Käyttäjäryhmissä voidaan myös luoda ryhmien alle tarkentavia ryhmiä.

Seuraavaksi luodaan käyttäjä, joka asetetaan ryhmään Hallinta. Käyttäjille voidaan määrittää erilaisia asioita, kuten vaihdetaanko salasana seuraavalla kirjautumisella tai lukitaanko tunnus automaattisesti jonain tiettynä päivänä. Määräaikaisien työntekijöiden kohdalla tätä voidaan hyödyntää, niin ACS-palvelimelle ei jää turhaan avonaisia tunnuksia työsuhteen päätyttyä. Alla esitetään kuinka käyttäjätunnus luodaan ja lisätään tiettyyn käyttäjäryhmään.



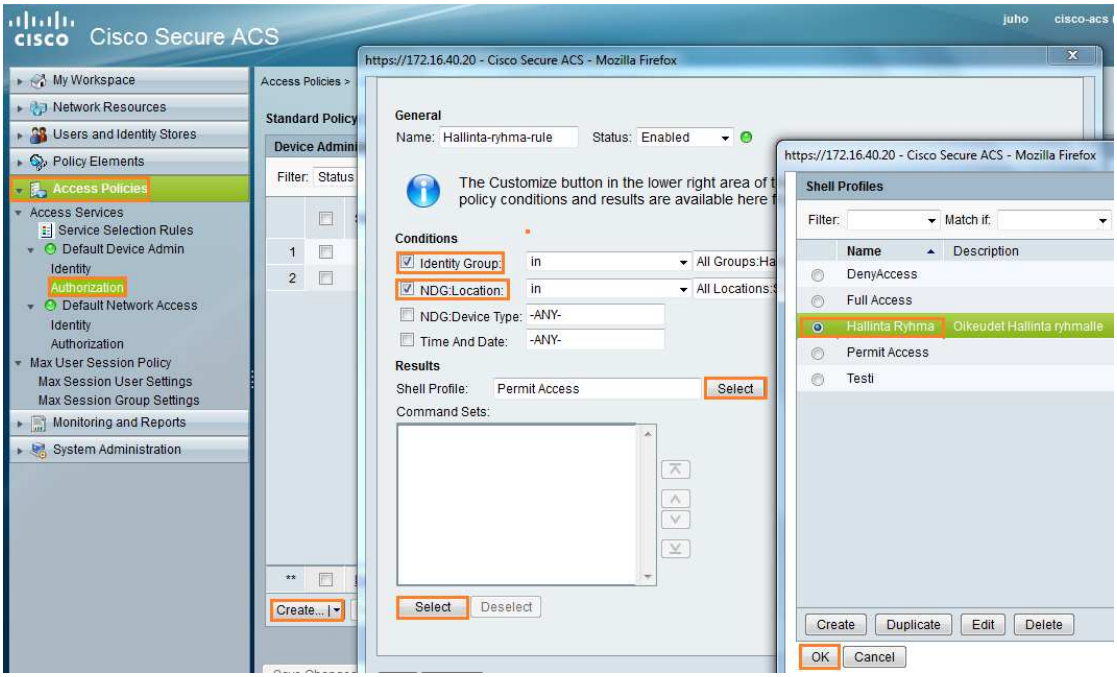
Käyttäjän lisääminen ja liittäminen ryhmään

Jotta käyttäjät voivat tehdä haluttuja asioita verkkolaitteille on niille luotava profiili, jossa määritetään halutut oikeustasot. Seuraavassa kuviossa on luotu hallinta ryh-

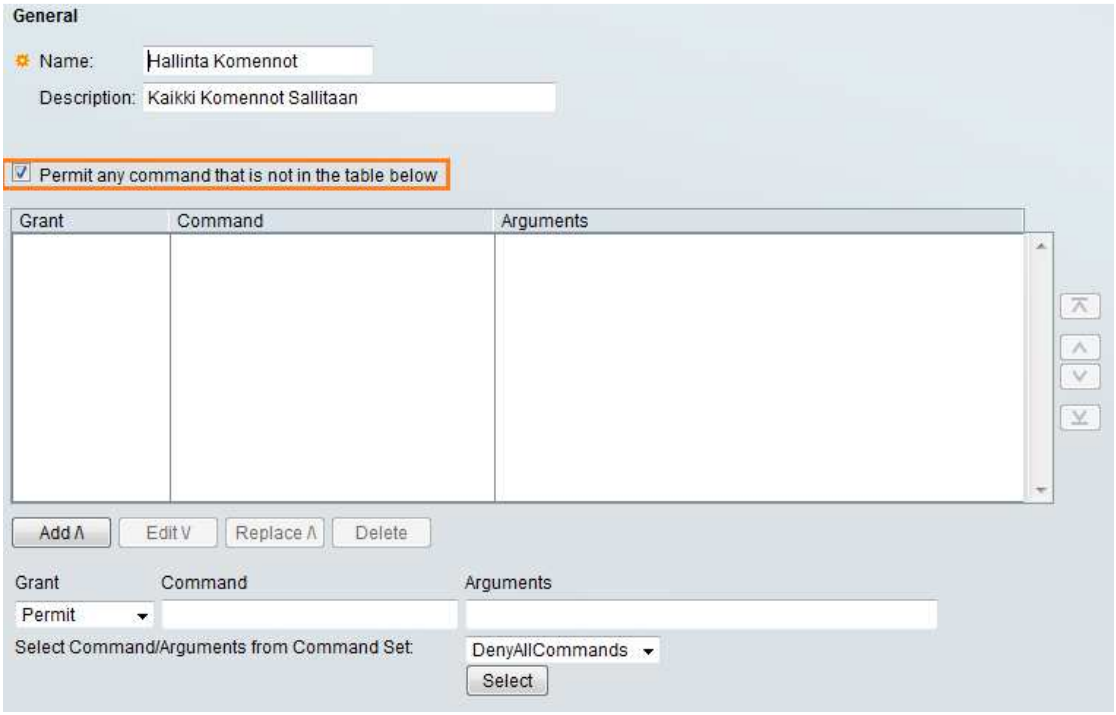
mälle profiili ja tälle on annettu korkein oikeustaso (Privilege 15). Kuvioon on liitetty ”*common tasks*”-osio.

Oikeuksia varten profiilin luominen

Seuraavaksi luodaan sääntö joka sitoo halutun profiilin haluttuun käyttäjäryhmään, eli valtuutetaan (*Authorization*) tietyt henkilöt tekemään tiettyjä asioita. Tässä vaiheessa voidaan määrittää minkä alueen laitteita, minkä laiteryhmän laitteita kyseinen ryhmä voi hallita tai valvoa. ”*Command Sets*”-kohtaan valitaan vielä komennot joita käyttäjäryhmä saa suorittaa laitteille. Kahdessa seuraavassa kohdassa on esitetty kuinka edellä mainitut tapahtumat tehdään.

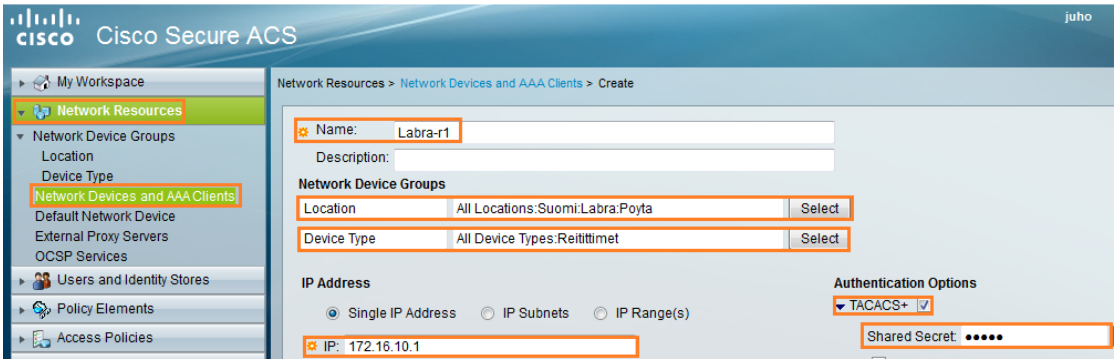


Valtuutuksen tekeminen käyttäjäryhmälle



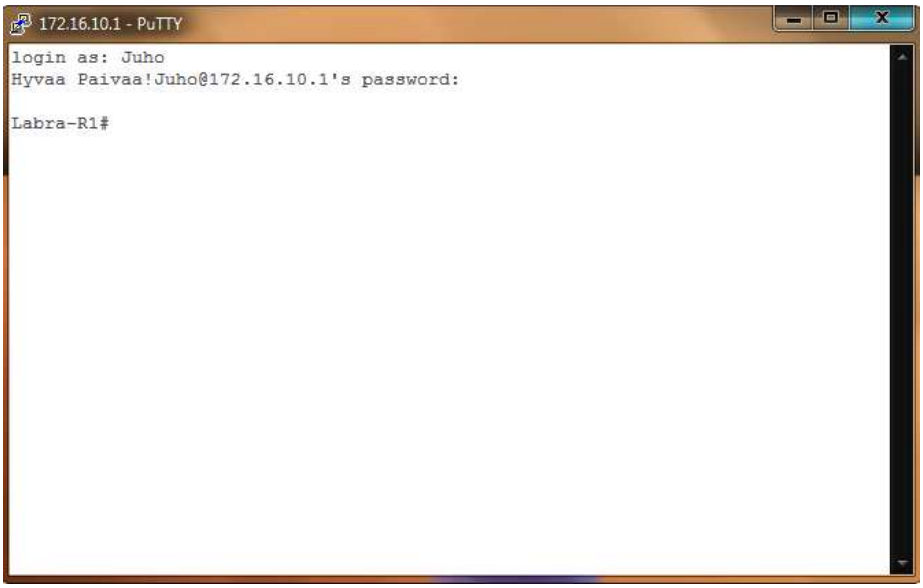
Command sets–valikko

Käyttäjät, jotka ovat hallintaryhmässä, ovat nyt valtuutettuja tekemään täyden oikeustason mukaisia asioita. Seuraavana on luotava ACS-palvelimelle asiakaslaite (NAS). Laitteelle määritellään sijainti sekä laiteryhmä, johon laite kuuluu. Laitteelle on määriteltävä myös IP-osoite ja autentikaatioon käytettävä protokolla, sekä protokollalle on määriteltävä jaettu salaisuus. Alla on näkymä tapahtumasta, jossa luodaan laite laboratorion pöydälle, ryhmään *Reitittimet* ja kyseinen laite asetetaan käyttämään autentikaatioon TACACS+-protokollaa.



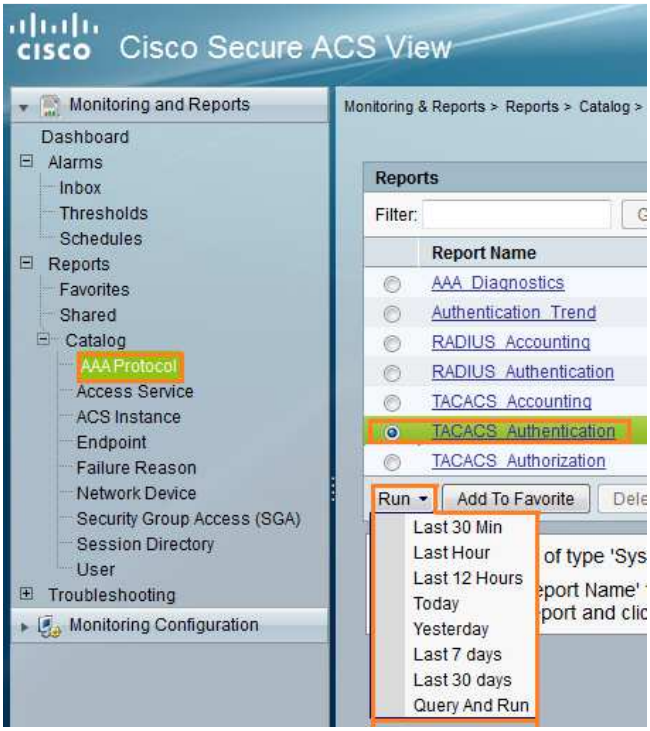
NAS-laitteen lisääminen ACS–palvelimelle

Kun kaikki edellä olleet asiat on määritelty, voidaan laitteelle ottaa yhteys tälle määritettyyn IP-osoitteeseen käyttäen SSH-protokollaa. Lopuksi on esitetty tapahtuma, jossa käyttäjä *Juho* on onnistunut autentikoitumaan Labra-r1-laitteelle suoraan *exec*-tilaan.



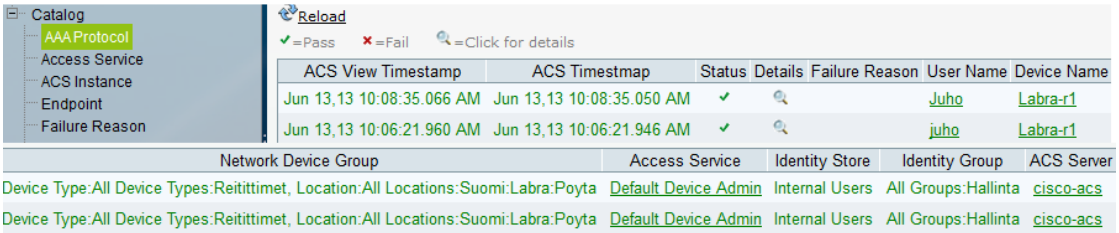
Onnistunut autentikointi NAS-laitteelle

AAA-arkkitehtuurista on nyt käsitelty tunnistautuminen ja valtuuttaminen. Seuraavaksi vuorossa on kirjanpito, joka on AAA-arkkitehtuurin viimeinen osa-alue. ACS-palvelimella ei voida vaikuttaa siihen mitä tietoja NAS-laitteet kirjaavat palvelimelle. ACS-palvelimella voidaan seurata tarkkojakin statistiikkoja kirjanpidosta, mikäli verkkolaitteet ovat konfiguroitu näitä kirjaamaan. ACS-palvelimen päävalikosta valitaan *”Monitoring and Reports”*-alavalikosta kohta *”Launch Monitoring and Repoter viewer*”. Selaimeen aukeaa uusi välilehti, jossa on erilaisia mahdollisuuksia seurata erilaisia hälytyksiä tai laitteiden lähettämiä kirjanpitotietoja. Kirjanpitotietoja voidaan selata myös halutulta ajalta, eli laitteelle ajansaatossa kerääntyneitä lokitietoja ei kaikkia tarvitse ladata näkymään. Seuraavassa kuviossa on esitetty kuinka pystytään valitsemaan AAA-arkkitehtuurin haluttu osa-ale ja tarkastelemaan sitä tietyltä ajanjaksolta.



AAA TACACS-autentikaatio lokitietojen tarkastelu halutulla aikavälillä

Seuraavaksi on esitelty miltä lokitiedot näyttävät ja mitä tietoja niistä on mahdollista saada. Kuviossa on kirjautumistapahtuma joka sisältää tiedon mihin aikaan käyttäjä *Juho* on autentikoitunut laitteelle *Labra-r1,* joka sijaitsee *Suomessa*, *labran pöydällä* ja on malliltaan *reititin* ja onko autentikaatio onnistunut. Tiedoista nähdään myös onko käyttäjän tunnistukseen käytetty sisäistä vai ulkoista käyttäjätietokantaa. Mikäli ACS-palvelimet olisivat klusterissa, eli niitä olisi useita, voidaan lokitietojen lopusta havaita ACS-palvelin, joka on suorittanut autentikaation.



TACACS+ -autentikaatioloki

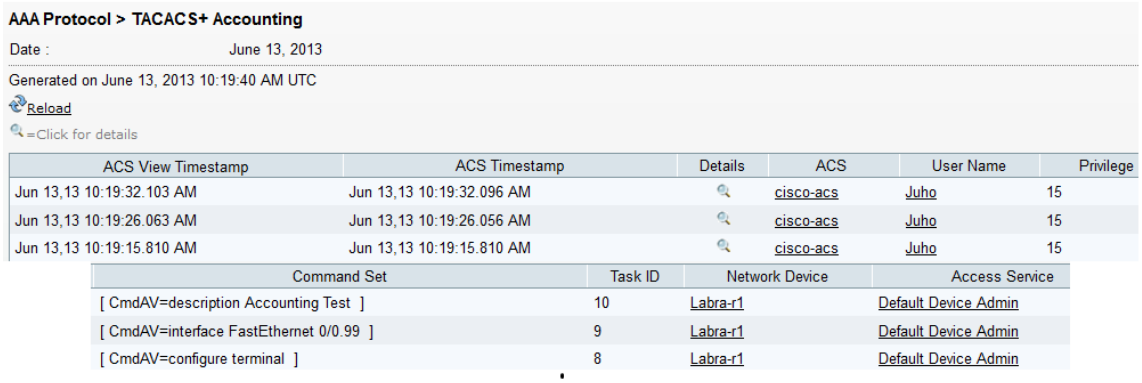
Edellä olevassa kuviossa näkyy *Details*-kohdassa suurennuslasi. Tästä painamalla saadaan näkyviin todella tarkkaa statistiikkaa tapahtumista, kuten askel askeleelta TACACS+-tapahtumat (*START-, REPLY-, CONTINUE*-viestit). Yksityiskohtaisista tiedoista, nähdään mm. seuraavanlaosiset yksityiskohtaiset tiedot pääsypolitiikasta, jolla käyttäjä on autentikoitunut.

Access Policy

Access Service:	Default Device Admin
Identity Store:	Internal Users
Selected Shell Profile:	Hallinta Ryhma
Active Directory Domain:	
Identity Group:	All Groups:Hallinta
Access Service Selection Matched Rule :	Rule-2
Identity Policy Matched Rule:	Default
Selected Identity Stores:	Internal Users, Internal Users
Query Identity Stores:	
Selected Query Identity Stores:	
Group Mapping Policy Matched Rule:	
Authorization Policy Matched Rule:	Hallinta-ryhma-rule
Authorization Exception Policy Matched Rule:	

Access Policy-tietoja.

Edellä esitelty asia ei suoranaisesti ole AAA-arkkitehtuurin kirjanpitoa, vaikka ACS-palvelin on nämä kirjannut ylös. *AAA Protocol*-kohdasta valittaessa *TACACS+ Accounting,* päästään näkemään mitä tietoja TACACS+ asiakaslaitteet ovat lähettäneet ACS-palvelimelle kirjattavaksi. *TACACS+ Accounting*-osiota voidaan myös lukea halutulta aikaväliltä, aivan kuten autentikaatiota. Seuraavassa kuviossa on näkymä, jossa käyttäjä *Juho* on luonut alirajanpinnan *Fastethernet 0/0.99* sekä määrittänyt tälle rajapintakuvaukseksi *Accounting Test*.



AAA Protocol > TACACS+ Accounting

Date : June 13, 2013

Generated on June 13, 2013 10:19:40 AM UTC

Reload

=Click for details

ACS View Timestamp	ACS Timestamp	Details	ACS	User Name	Privilege
Jun 13,13 10:19:32.103 AM	Jun 13,13 10:19:32.096 AM		cisco-acs	Juho	15
Jun 13,13 10:19:26.063 AM	Jun 13,13 10:19:26.056 AM		cisco-acs	Juho	15
Jun 13,13 10:19:15.810 AM	Jun 13,13 10:19:15.810 AM		cisco-acs	Juho	15

Command Set	Task ID	Network Device	Access Service
[CmdAV=description Accounting Test]	10	Labra-r1	Default Device Admin
[CmdAV=interface FastEthernet 0/0.99]	9	Labra-r1	Default Device Admin
[CmdAV=configure terminal]	8	Labra-r1	Default Device Admin

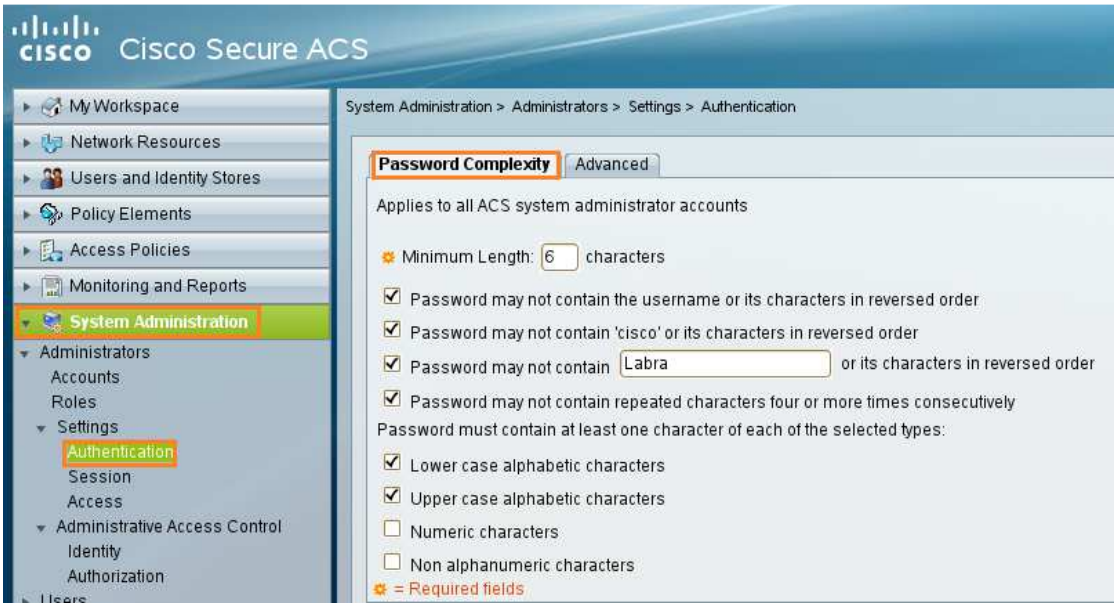
TACACS+ kirjanpito komennoista

ACS-palvelimelle voidaan luoda käyttäjiä, joilla on mahdollisuus kirjautua itse palvelimelle. Palvelimella voidaan käyttäjille määrittää seuraavanlaisia oikeuksia.

ACS Roolit

Yllä olevasta kuviossa on esitelty kaikki roolit, joita käyttäjille voidaan määrittää, mutta yleisimmät ovat pääkäyttäjät (*SuperAdmin*), eli käyttäjät, jotka voivat tehdä konfiguraatio muutoksia itse palvelimelle, sekä lukuoikeudet joko monitorointi puolelle (*ReportAdmin*) tai vaihtoehtoisesti koko palvelimelle lukuoikeus (*ReadOnlyAdmin*).

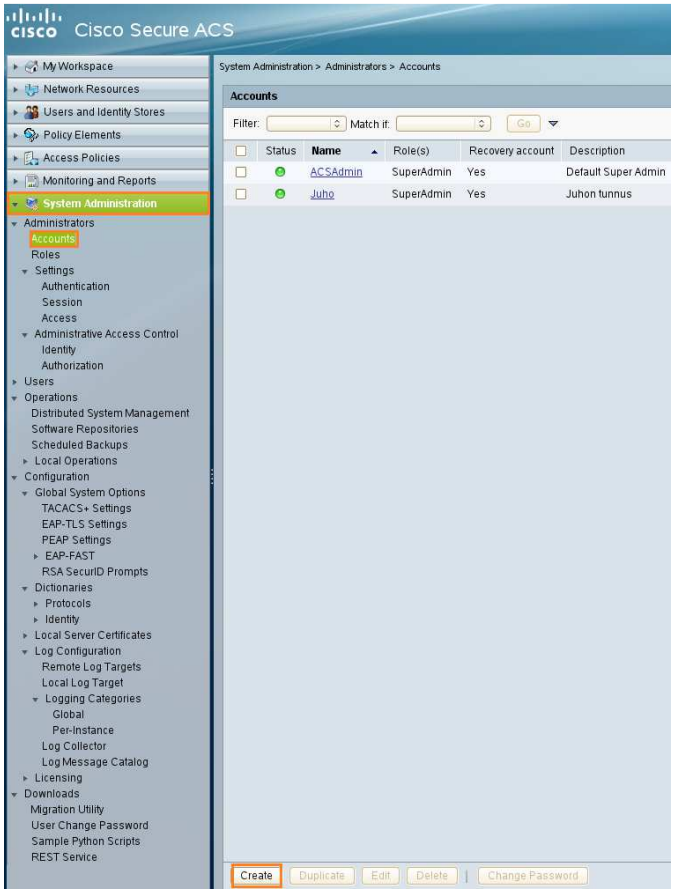
Salasanapolitiikkaa on myös hyvä vaihtaa ACS-palvelimelle, sillä oletuksena salasana vaatimus on 4 merkkiä ja sillä ei ole sisältö vaatimuksia. Seuraavaksi on esitelty, kuinka salasanapolitiikkaa voidaan koventaa.



Salasanapolitiikan koventaminen

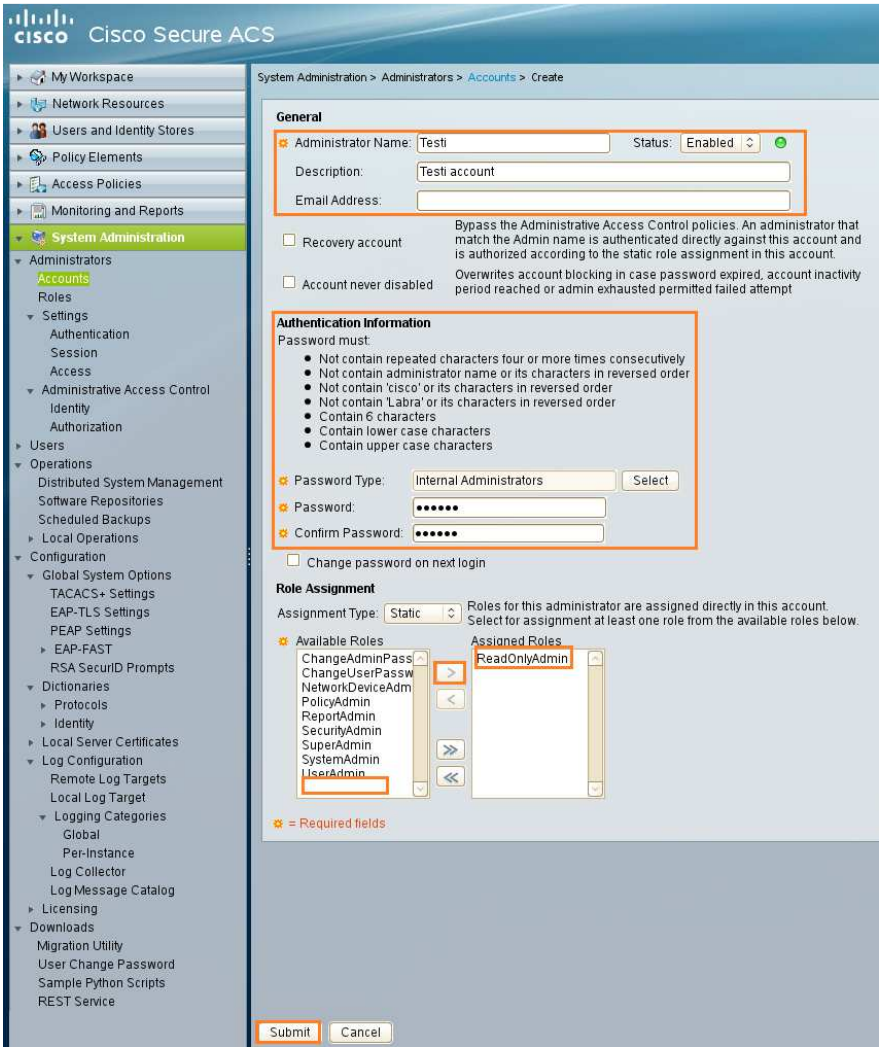
Edellä olevasta kuviosta voidaan havaita, että salasanan pituus on vaihdettu kuuteen merkkiin. Salasana ei saa sisältää käyttäjänimeä tai merkkijonoa samanlaisessa järjestyksessä. Salasana ei saa sisältää merkkijonoa *cisco* tai merkkijonoa samanlaisessa järjestyksessä. Salasana ei saa sisältää merkkijono *Labra* tai merkkijonoa samanlaisessa järjestyksessä. Salasana ei saa sisältää neljää tai useampaa samaa merkkiä peräkkäin sekä salasanassa tulee olla vähintään yksi pieni- ja isokirjain.

Salasanapolitiikan koventamisen jälkeen voidaan ryhtyä luomaan käyttäjiä itse ACS-palvelimelle, henkilöille joille halutaan valtuuttaa pääsy itse palvelimelle. Seuraavaksi on esitetty miten päästään luomaan ACS-käyttäjiä.



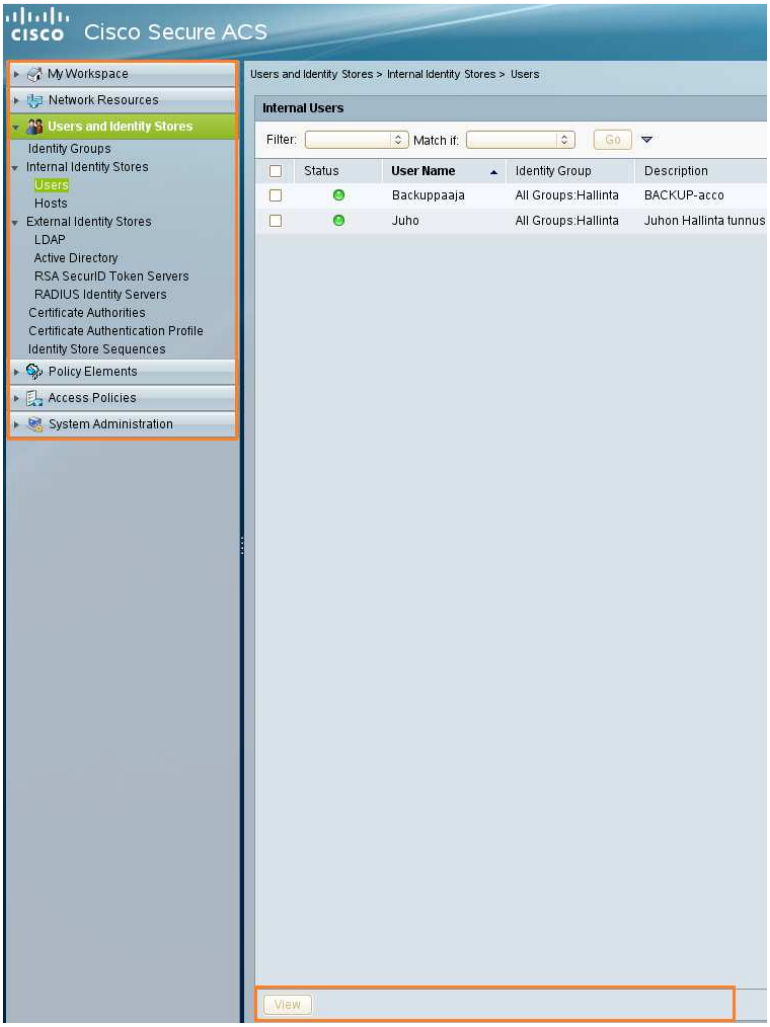
ACS – käyttäjän lisääminen osa 1

Seuraavaksi määritetään käyttäjälle ominaisuuksia kuten nimi, kuvaus, salasana ja rooli. Kyseinen tapahtuma on esitelty seuraavassa kuviossa.



ACS – käyttäjän lisääminen osa2

Edellä olevasta kuviosta havaitaan, että salasanapolitiikka on voimassa ja että kyseiselle käyttäjälle on lisätty rooli ”*ReadOnlyAdmin*” eli kyseinen henkilö pääsee ainoastaan tarkkailemaan ACS-asetuksia, kuten seuraavasta kuviosta voidaan havaita.

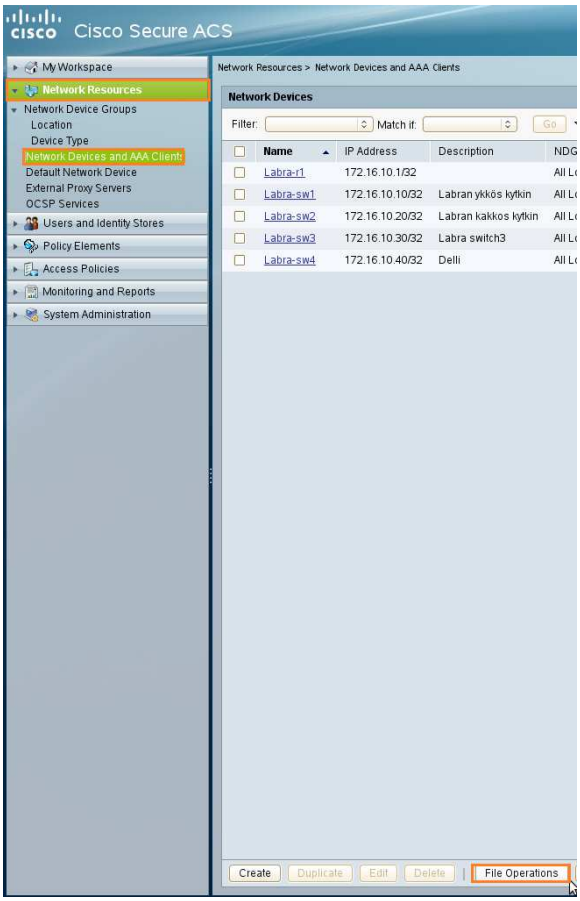


Kirjautuminen Testi käyttäjällä ACS–palvelimelle

Kuten edellä olevasta kuviosta voidaan havaita, ei aikaisemmin luotu käyttäjä pääse tekemään muutoksia palvelimelle, sillä alareunasta puuttuu kokonaan ”*create*”-painike, ainoastaan ”*view*”-painike on tallella, josta voidaan tarkastella esimerkiksi käyttäjiä. Vasenta laitaa tarkastellessa huomataan, ettei kyseisellä käyttäjällä ole myöskään mahdollista päästä lukemaan lokitapahtumia sillä ”*Monitoring and Reports*”-välilehti puuttuu kokonaan.

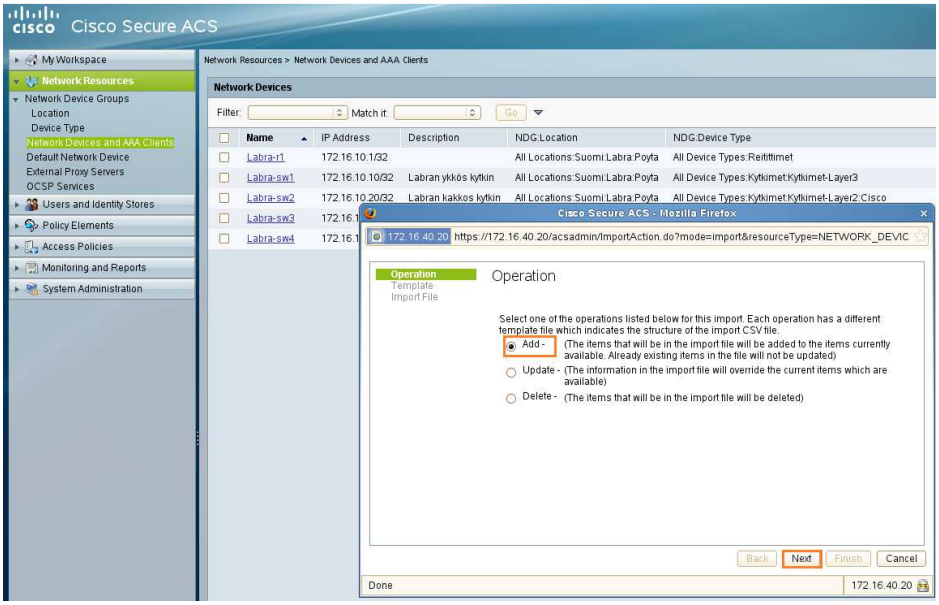
Useiden verkkolaitteiden lisäämiseen on syytä käyttää erillistä tiedostoa, jotta verkkolaitteiden lisäämiseen ei kuluisi aikaa todella paljoa. Opinnäytetyön yhteydessä oli laitteet jo määritelty käsin ACS-palvelimelle mutta mikäli laboratorioympäristöön tulisi useita laitteita lisää, on kyseiset laitteet mahdollista lisätä yhden tiedoston avul-

la. Alla olevan kuvion mukaisesti valitaan AAA-asiakkaiden lisäys ikkunasta *"File Operations"*.



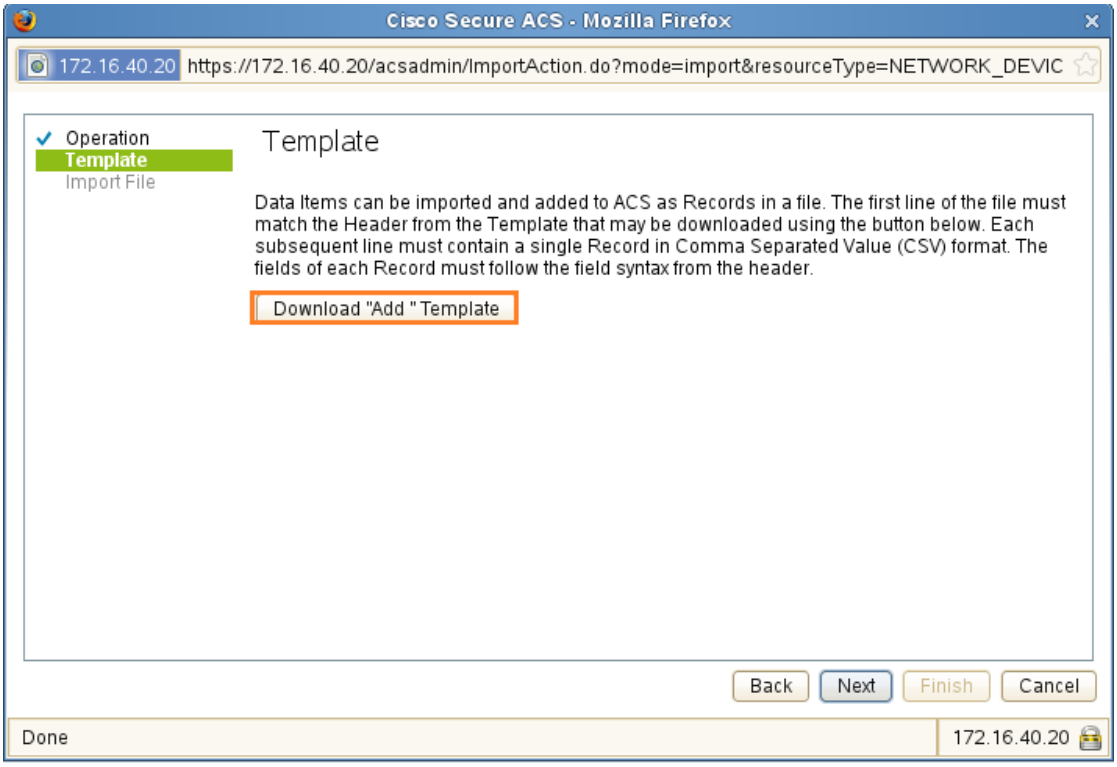
ACS File Operations

Mikäli ACS-palvelimelle halutaan viedä uusia verkkolaitteita, niin valitaan valikosta *Add*-kohta. Valikosta on myös mahdollista valita muutokseen sekä poistoon tarkoitetut kohdat (*Update & Delete*) seuraavan kuvion mukaisesti.



ADD -valinta

Seuraavaksi ikkunassa avautuu alla olevan kuvion mukainen tapahtuma, josta valitaan *Download ”Add” Template*.



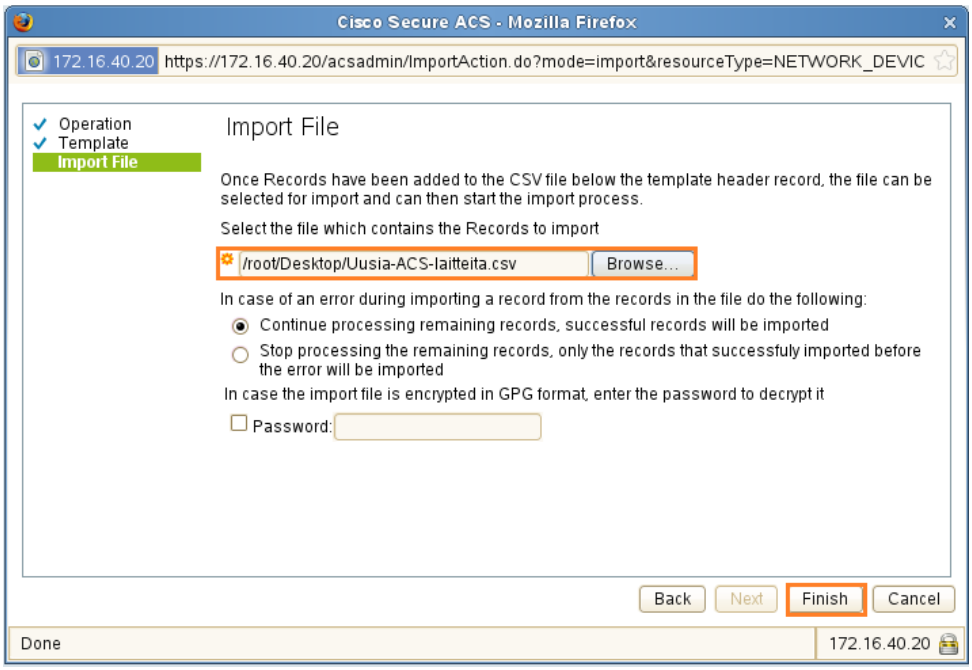
Add Template

Kun *.csv*-tiedosto on ladattu, pitää sitä hieman muuttaa jotta saadaan järkevän näköinen ja helppolukuinen *notepad*-tiedosto. Kyseisen operaation kerran tehtyä, kannattaa tiedosto tallentaa muistiin, jotta samaa pohjaa voidaan hyödyntää jatkossakin. Seuraavaksi on esitetty miltä muokattu notepad-tiedosto näyttää laite lisäyksineen. (Tiedostossa olevat erilliset asiat tulee olla yhtäjaksoisia, jotta tiedosto toimii, kuvioon lisätty rivinvaihtoja selkeyden vuoksi.)

```
name:String(64):Required,description:String(1024),"subnets:Subnets(a.b.c.d/m; a:b:c:: ..., excluding a.b.c.d/32
;... wild cards IPv4 (*,-) IPv6 (:,::) exclude range is optional for IPv4 only):Required","supportRADIUS:
Boolean(true,false):Required",radiusSecret:String(32),coaPort:Integer,"supportKeyWrap:Boolean(true,false)"
,keywrapKEK:String(32),keywrapMACK:String(40),"keywrapDisplayInHex:Boolean(true,false)","supportTACACS:
Boolean(true,false):Required",tacacsSecret:String(32),"singleconnect:Boolean(true,false)","legacyTACACS:
Boolean(true,false)",Location:String(256),Device Type:String(256)
Labra-sw5,testi,172.16.10.50/32,false,,,false,,,false,true,labra,true,true,All Locations:Suomi:
Labra:Poyta,All Device Types:Kytkimet:Kytkimet-Layer2:Cisco
Labra-sw6,testi,172.16.10.60/32,false,,,false,,,false,true,labra,true,true,All Locations:Suomi:
Labra:Poyta,All Device Types:Kytkimet:Kytkimet-Layer2:Cisco
Labra-sw7,testi,172.16.10.70/32,false,,,false,,,false,true,labra,true,true,All Locations:Suomi:
Labra:Poyta,All Device Types:Kytkimet:Kytkimet-Layer2:Cisco
Labra-sw8,testi,172.16.10.80/32,false,,,false,,,false,true,labra,true,true,All Locations:Suomi:
Labra:Poyta,All Device Types:Kytkimet:Kytkimet-Layer2:Cisco
Labra-sw9,testi,172.16.10.90/32,false,,,false,,,false,true,labra,true,true,All Locations:Suomi:
Labra:Poyta,All Device Types:Kytkimet:Kytkimet-Layer2:Cisco

Labra-sw10,testi,172.16.10.100/32,false,,,false,,,false,true,labra,true,true,All Locations:Suomi:
Labra:Poyta,All Device Types:Kytkimet:Kytkimet-Layer3
Labra-sw11,testi,172.16.10.110/32,false,,,false,,,false,true,labra,true,true,All Locations:Suomi:
Labra:Poyta,All Device Types:Kytkimet:Kytkimet-Layer3
Labra-r12,testi,172.16.10.120/32,false,,,false,,,false,true,labra,true,true,All Locations:Suomi:
Labra:Poyta,All Device Types:Reitittimet
```

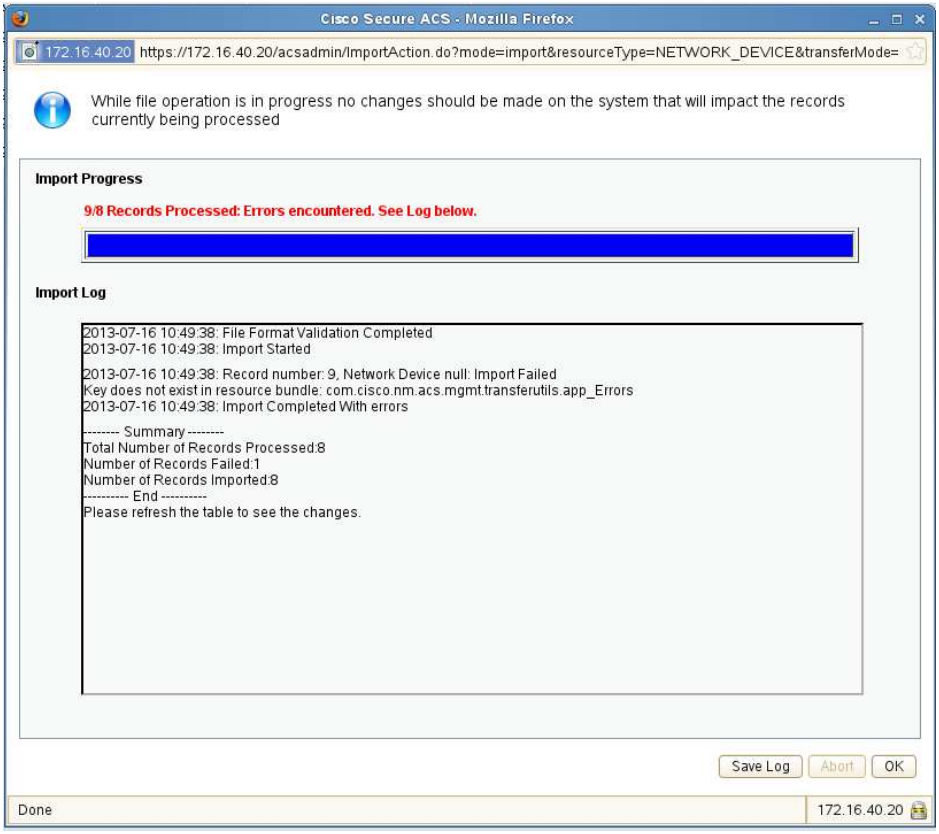
.csv-tiedosto laitteiden lisäämistä varten

Seuraavaksi palataan takaisin ACS-palvelimelle jossa luotu *.csv*-tiedosto ladataan palvelimelle. Tapahtuma on esitelty alla.



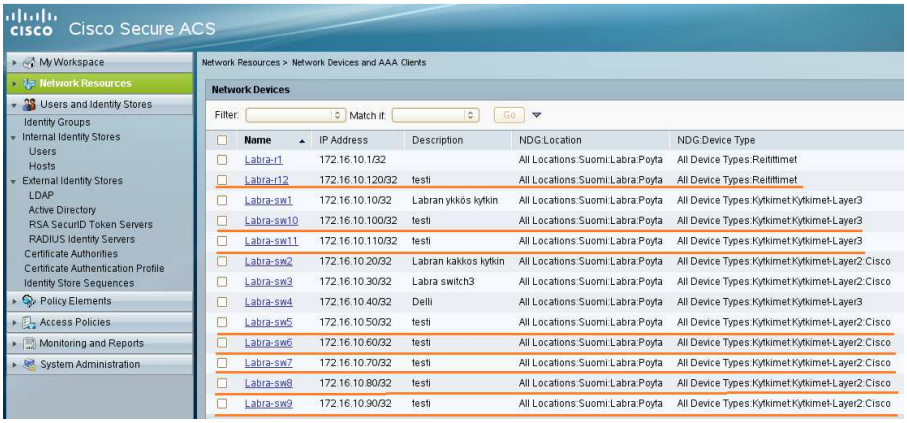
Lisätään tiedosto laitteiden lisäystä varten

Seuraavaksi huomataan, että lisäys onnistui.



Onnistunut laitteiden tuominen

Edellä olevassa kuviossa on yksi epäonnistunut laitteen vienti. Työssä ei keksitty selitystä sille, miksi ACS-palvelin luuli, että laitteita on 9 vaikka todellisuudessa niitä oli .cvs-tiedostossa 8 kuten seuraavasta kuviosta voidaan laskea (sw-5 – 11 + r12 = 8kpl). Lopuksi ACS-palvelimen välilehti tulee päivittää, jonka jälkeen voidaan havaita, että laitteet ovat lisääntyneet, aivan kuten pitikin. (ks. Kuvio 132)

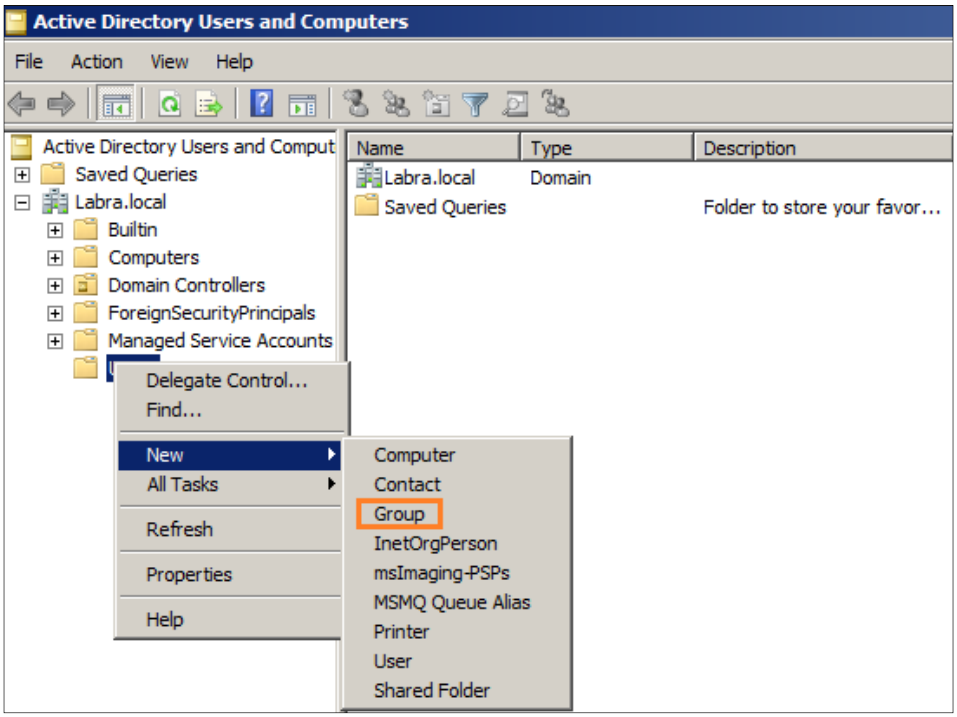


Päivittynyt laiteluettelo

Liite 4. Toimeksiantajalle ohje ACS- ja Windows AD-palvelimien integroimiseen

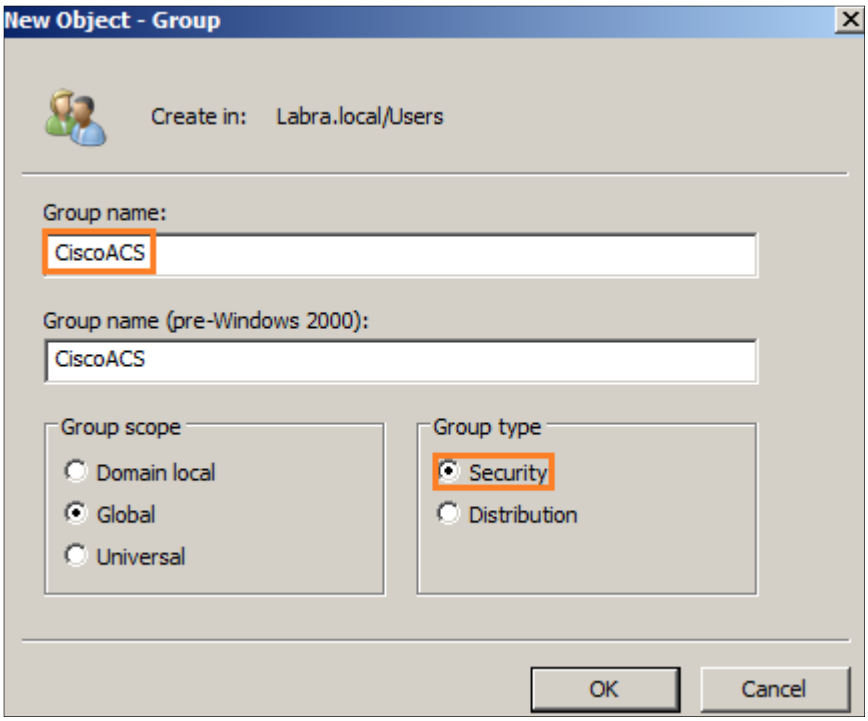
Kuten edellisessä liitteessä muutokset on otettava aina käyttöön, joko *submit*-painikkeella tai *Save Changes*-painikkeella. Luodessa esimerkiksi käyttäjiä tai sääntöjä ACS-palvelimelle voidaan ne määrittää käyttöön asettamalla ne *enable*-tilaan ja vastaavasti määrittää ne käyttämättömäksi asettamalla ne *disable*-tilaan.

AD-palvelimelle luodaan käyttäjäryhmä. Seuraavaksi on esitetty mistä ryhmä lisätään.



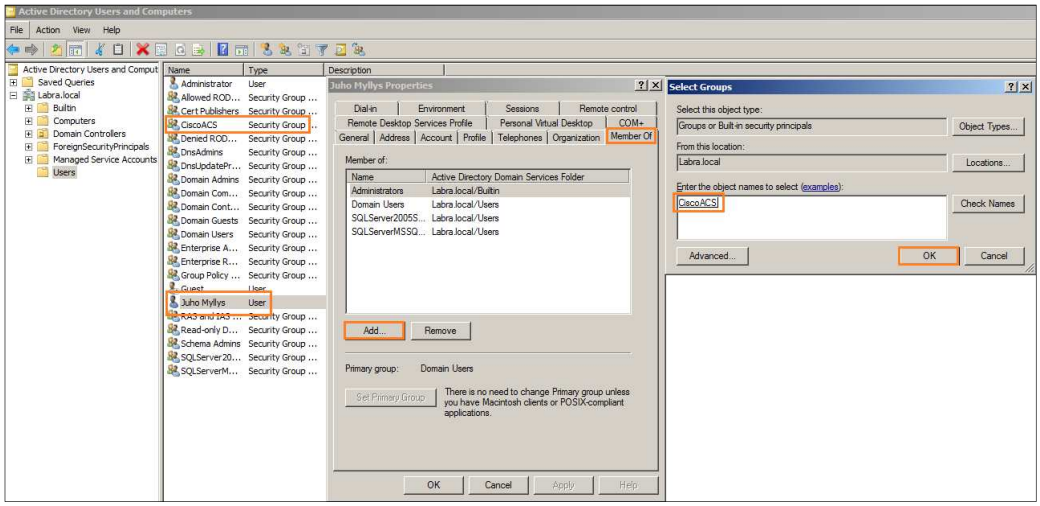
Navigointi AD-palvelimen ryhmän lisäykseen

Seuraavaksi luodaan *securitygroup* nimeltä CiscoACS. Alla on esitetty ryhmän lisääminen.



AD:lle ryhmän lisääminen

Seuraavassa kuviossa on esitetty vaiheittain käyttäjän *Juho Myllys* lisääminen aiemmin luotuun ryhmään *CiscoACS*.



Käyttäjän lisääminen ryhmään

Yllä olevassa kuviossa on muokattu käyttäjän *Juho Myllys* asetuksia välilehdestä *Member Of*, jossa tämä on määritetty aiemmin luodun *CiscoACS* ryhmän jäseneksi. Lopuksi varmistetaan vielä, että ryhmässä *CiscoACS* on jäsenenä *Juho Myllys*.

AD-palvelimelle käyttäjäryhmän ja käyttäjän liitoksen jälkeen tarkastetaan vielä AD-toimialueen nimi. Toimialueen voi tarkastaa esimerkiksi kysymällä verkon ylläpidolta tai tietokoneelta katsomalla *Ohjauspaneeli* → *Kaikki ohjauspaneelin kohteet* → *Järjestelmä* ja sieltä kohdasta *Tietokoneen nimen*, *toimialueen ja työryhmän asetukset* → *Toimialue*: (Windows). Kun toimialue on tiedossa, voidaan aloittaa ACS-palvelimen liittämistä AD-palvelimeen.

ACS-palvelimeen otetaan ensimmäisenä SSH-yhteys ja määritellään aikavyöhyke sekä NTP-palvelin. Koska harjoitusympäristössä ei ollut mahdollista käyttää erillistä NTP-palvelinta, luotiin se AD-palvelimelle. Kun SSH-yhteys on muodostunut ACS-palvelimelle konfiguroidaan globaalissa konfiguraatio tilassa NTP-palvelin komennolla: (Cisco Systems ACS 5.x and later integration with Microsoft Active Directory Configuration, 2013)

#clock timezone UTC/2+

#ntp server 172.16.40.10

NTP-palvelin määrityksen jälkeen laite täytyy käynnistää uudelleen. Edellä olevat muutokset on hyvä tarkistaa komennoilla:

#show clock

#show timezone

ACS-palvelimelle voidaan määrittää nimipalvelin, joka vastaa toimialueen nimikyselyihin. ACS-palvelimen asennuksen yhteydessä palvelimelle määritetään vähintään yksi nimipalvelin. Mikäli nimipalvelin vaihdetaan niin, tulee se tehdä komennolla:

#ip name-server 172.16.40.10

Tämän jälkeen voidaan kokeilla DNS-kyselyllä nimipalvelimen toimintaa. Alla on suoritettu *DNS*-kysely toimialueenohjaimen nimeä varten: (Cisco Systems ACS 5.x and later integration with Microsoft Active Directory Configuration, 2013)

```
cisco-acs/admin# nslookup labra.local
Trying "labra.local"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 37353
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; QUESTION SECTION:
;labra.local.                   IN      ANY

;; ANSWER SECTION:
labra.local.            600     IN      A       172.16.40.10
labra.local.            3600    IN      NS      winkkarir2.labra.local.
labra.local.            3600    IN      SOA     winkkarir2.labra.local. hostmaster.labra.local. 175 900 600 86400 3600

;; ADDITIONAL SECTION:
winkkarir2.labra.local. 3600    IN      A       172.16.40.10

Received 133 bytes from 172.16.40.10#53 in 1 ms

cisco-acs/admin#
```

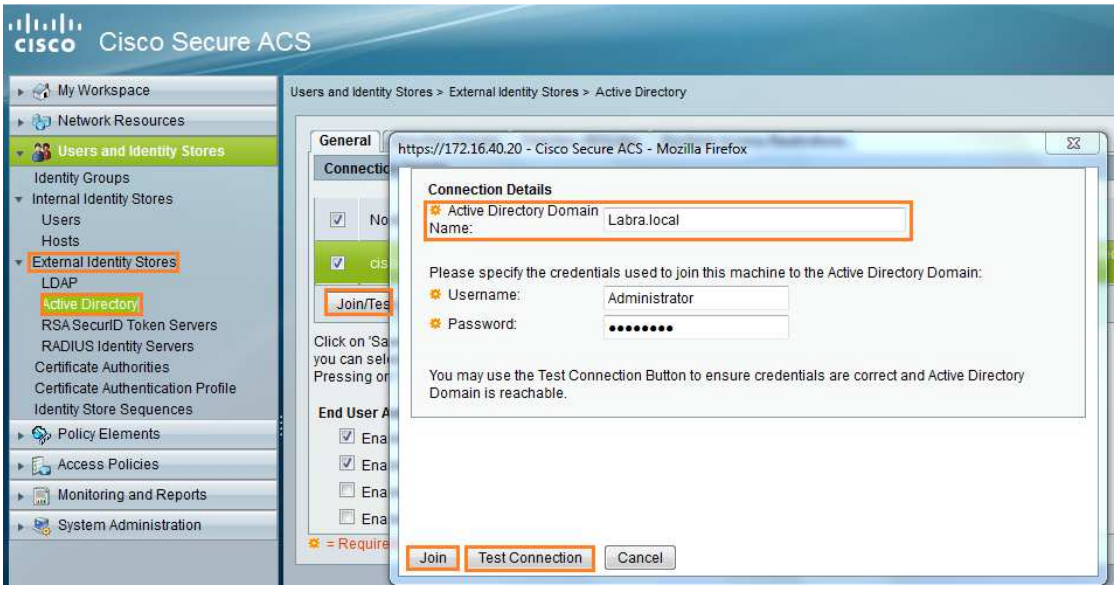
ACS-palvelin nslookup-komento

Edellä tehtyjen muutosten jälkeen pitää palomuuriin, mikäli sellainen on ACS ja AD-palvelimien välissä, tehdä avauksia jotta ACS-palvelin pystyy liittymään toimialueeseen. Seuraavaksi on listattu tieto siitä, mitä palveluita tarvitaan, mitä porttia palvelu käyttää ja mitä kuljetusprotokollaa se käyttää.

Palomuuriavaukset ACS → AD

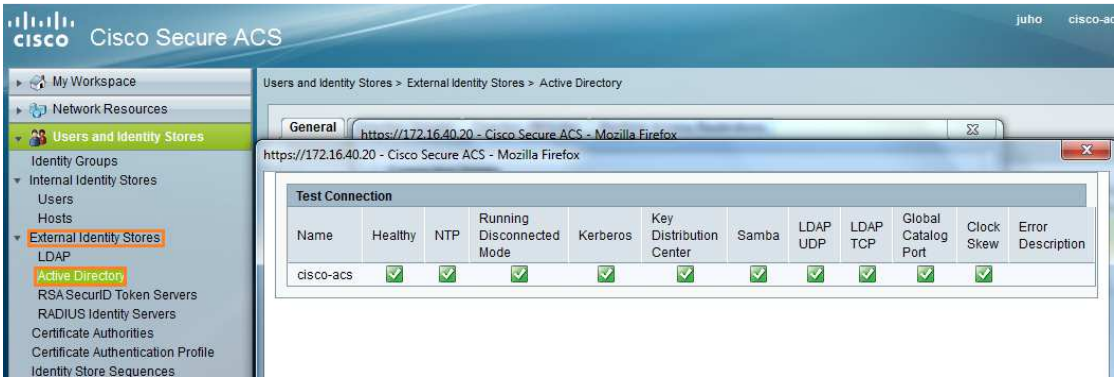
Palvelu	Kuljetusprotokolla	Portti
LDAP	UDP & TCP	389
KDC	TCP	88
KPASSWD	TCP	464
NTP	UDP	123
GLOBAL CATA-LOUGE	TCP	3268
DNS	UDP	53
SAMBA	TCP	389

Palomuuriavausten jälkeen ja *ACS*-määritysten jälkeen voidaan ryhtyä itse AD-liitoksen tekemiseen. Ensimmäisenä on hyvä testata ACS-palvelimella yhteyttä AD-palvelimeen. Seuraavana on esitelty tapahtuma, jossa määritetään toimialueen tiedot.



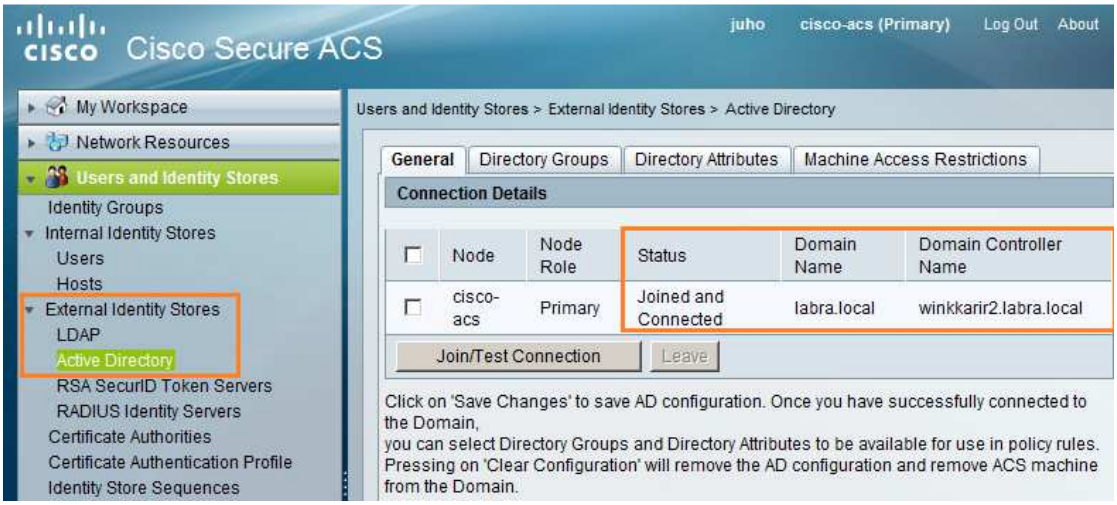
Toimialue määritykset

Seuraavassa kuviossa on valittu *Test Connection* eli yhteystesti AD-palvelimeen.



ACS ja AD-palvelimien yhteystesti

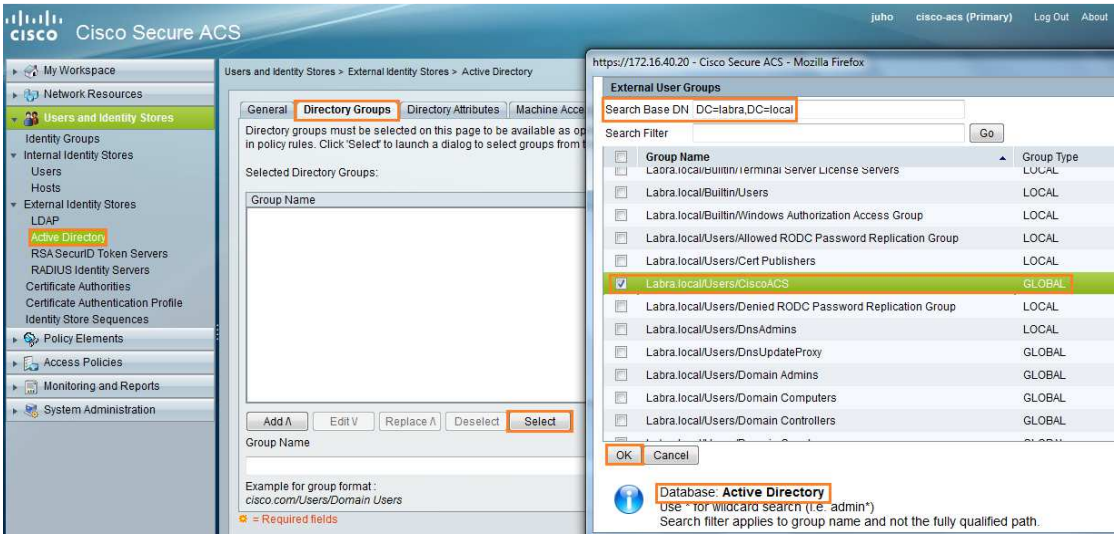
AD-palvelimelle määritetään *External Identity Stores* kohdasta *Active Directory*. Palvelimelle määritetään toimialue johon halutaan liittyä tai vaihtoehtoisesti tehdä yhteystesti. Mikäli toimialueeseen halutaan liittyä, on AD-palvelimelle määriteltävä ACS-tunnus tai liityttävä jollain voimassa olevalla tunnuksella. Alla on yhteystestin sijaan valittu liittyminen toimialueeseen.



ACS-palvelimen liittäminen AD-palvelimeen

Kuten edellisestä kuviosta havaitaan, on *Status*-tila *Joined and Connected*. ACS-palvelin on liittynyt onnistuneesi toimialueeseen ”*labra.local*”. Kuviosta havaitaan toimialue ja toimialueenohjaimen nimi, joka on *winkkarir2.labra.local*.

AD-palvelimelle luotiin alussa ryhmä *CiscoACS*, seuraavaksi määritetään ACS-palvelin tunnistamaan käyttäjiä tästä ryhmästä. Seuraavana on AD-käyttäjäryhmän valinta.

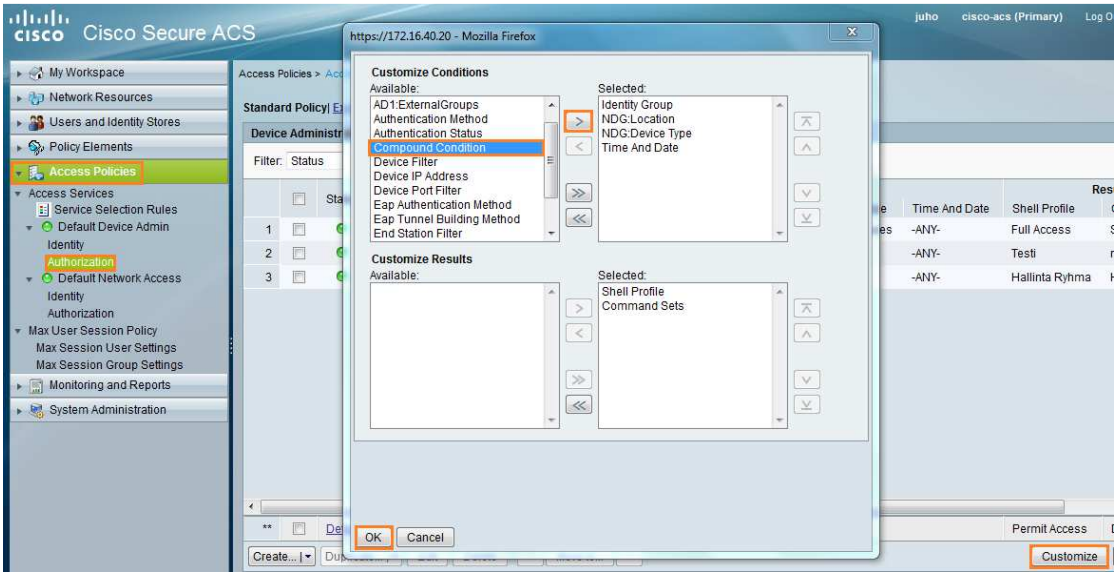


AD-palvelimen käyttäjäryhmän valitseminen

Seuraavaksi määritellään ACS-palvelin käyttämään AD-palvelinta käyttäjien tunnistamiseen. Alla otetaan AD-identifiointi käyttöön.

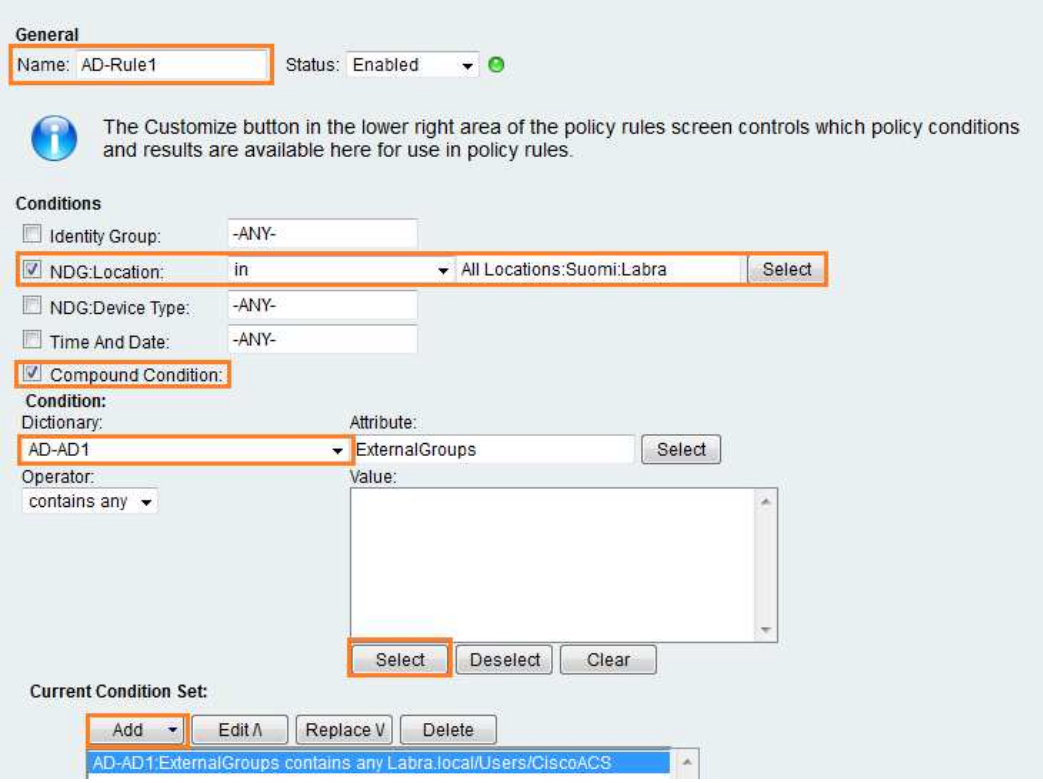
AD-tunnistautumisen määrittäminen

Seuraavaksi siirrytään valtuuttamiseen. Koska käytössä on ulkoinen käyttäjätietokanta, niin pitää valtuuttamista hieman kustomoida. Valtuuttamisen ehtoihin valitaan yhdiste, jonka avulla pystytään liittämään sääntöihin tieto, että kyseinen sääntö koskee AD-käyttäjiä. Alla olevassa kuviossa on esitetty miten valtuuttamiseen liittyviä valintoja voidaan muokata.



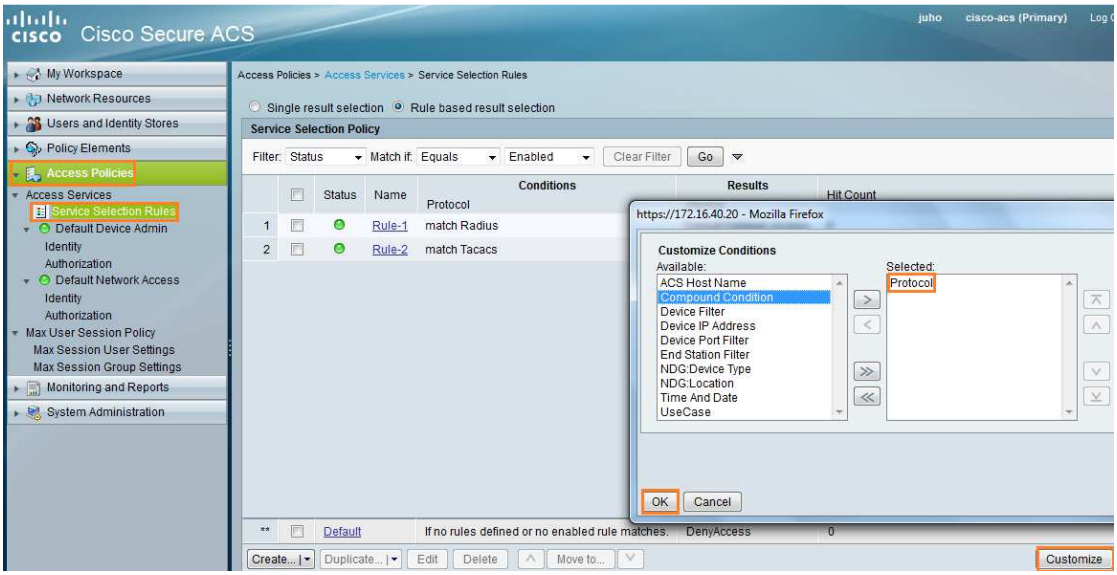
Valtuuttamista varten uuden yhdisteen lisääminen

Tämän jälkeen luodaan valtuuttamiseen itse sääntö, jossa määritellään säännölle nimi, mitä laitteita AD-käyttäjät voivat hallita sekä valitaan AD-palvelimelta käyttäjäryhmä ja heille asetetaan tietyt komennot käyttöön. Samaan tapaan AD-palvelimelle voisi tehdä ryhmän *ACS-valvonta*, jolle annettaisi vain lukuoikeudet laitteille. Sääntöä pääsee luomaan *Access Policies* → *Authorization* → *create*. Seuraavassa kuviossa on esitetty kuinka luodaan valtuuttamiseen AD-käyttäjille sääntö, kuvion ulkopuolella valitaan normaalisti vain komennot, jotka sallitaan kyseiselle AD-käyttäjäryhmälle. Komentojen määrittäminen tapahtuu vastaavasti kuin liitteessä 3 on esitetty.



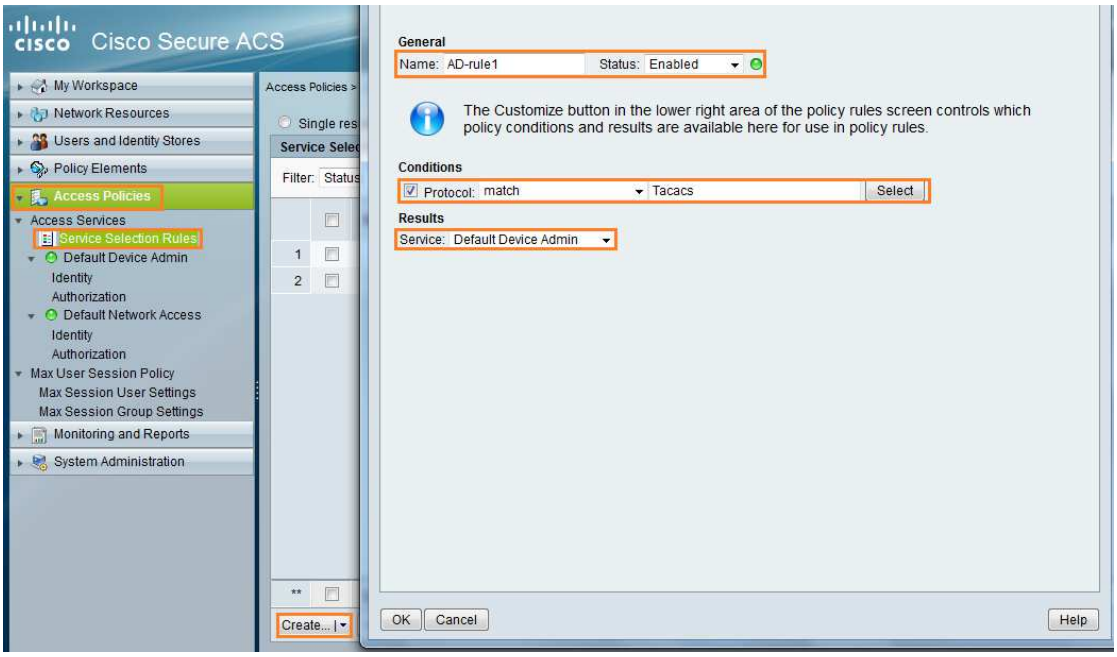
AD-käyttäjille valtuuttaminen

Lopuksi valitaan autentikaatioprotokolla, joka liitetään verkkolaitteille kirjautuviin henkilöihin. Alla olevassa kuviossa varmistetaan, että yhdistettäväksi tekijäksi on mahdollista valita protokolla. Komentojen valtuuttaminen tapahtuu vastaavalla tavalla kuin sisäisille käyttäjille.



Protokollan varmistaminen yhdisteeksi

Luodaan sääntö nimeltä *AD-rule1*, jossa määritetään laitteille kirjautuville henkilöille protokollaksi *TACACS*. seuraavana on esitelty säännön luonnista esimerkki.



Kirjautumiseen käytettävän protokollan määrittäminen

Lopuksi voidaan kirjautua verkkolaitteelle AD-tileillä, jotka ovat valtuutetussa ryhmässä AD-palvelimella.

Liite 5. Konfiguraatioiden suorittamista varten luotu skripti

```
#!/bin/bash -x
#määritellään lokitiedosto
LOGFILE=/home/juho/ONT-MENU.log
#Aliohjelma nimeltä log, jonka tehtävänä on määrittää lokiviestit lokitiedostoon
log()
{
PVM=`date +"%Y.%m.%d %H:%M:%S"`
echo "$PVM $1" >>$LOGFILE
}
#luodaan muuttujia
SWnimet=`grep -Eo '172\.16\.[0,1,6,4]{1,2}\.[0-9]{1,3}' /etc/hosts`
PVMbu=`date +%d.%m.%y_Ajassa_%H:%M`
```

```
HPJONO=iso.3.6.1.4.1.11
DELLJONO=iso.3.6.1.4.1.674
CISCOJONO=iso.3.6.1.4.1.9
#Luodaan aliohjelma nimeltä toiminnot jossa käydään SWnimet muuttujan keräämät nimet läpi kysyen SysOIDia snmpwalk-komennolla ja tulosten perusteella tehdään joko cisco, dell tai hp toimintoja.
toiminnot()
{
for i in $SWnimet
do
SWValmistaja=`snmpwalk -c $community -v2c -t 1 $i 1.3.6.1.2.1.1.2`
#Jos on valittu valmistajaksi cisco ja SNMP-kysely löytää muuttujan ciscojono, niin hypätään aliohjelmaan “CiscoToiminnot” ja suoritetaan sitä osoitteella “i”
case $VALM in
        CISCO)
        CISCO=`echo $SWValmistaja|grep -c $CISCOJONO`;
        if [ $CISCO -gt 0 ]; then
        CiscoToiminnot $i
#Koodi ei aina ole täysin vakaa, eli lokitetaan jos jotain ihmeellistä käy
else
                log "IP-osoitteelle $i ei loytynyt valmistajaa $VALM tai IP-osoitteeseen $i ei saada yhteytta!"
        fi
        ;;
#Jos valinta on Dell, suoritetaan vastaavasti Dellin laitteelle konfiguraatiot
        DELL)
        DELL=`echo $SWValmistaja|grep -c $DELLJONO`
        if [ $DELL -gt 0 ]; then
                DellToiminnot $i
        else
                log "IP-osoitteelle $i ei loytynyt valmistajaa $VALM tai IP-osoitteeseen $i ei saada yhteytta!"
        fi
        ;;
#HP:lle sama kuin kaksi yllä olevaa
HP)
        HP=`echo $SWValmistaja|grep -c $HPJONO`
        if [ $HP -gt 0 ]; then
                HPToiminnot $i
        else
```

```
                    log "IP-osoitteelle $i ei loytynyt valmistajaa $VALM tai IP-
osoitteeseen $i ei saada yhteytta!"
        fi
        ;;
#Muissa tapahtumissa lokitetaan virhe
*)
                    log "Virheellinen valmistajakoodi $VALM"
esac
done
}
# Cisco laitteiden toiminnot
CiscoToiminnot ()
{
#määritellään muuttuja laite, joka on siis IP-osoite, jolla ajettiin ciscotoiminnot.
Sana laite on selkeämpi vaihtoehto kuin ”$1”.
laite=$1
#Luodaan muuttuja varmuuskopiointia varten, eli IP:tä vastaava nimi haetaan
/etc/hosts-tiedostosta, tiedosto voi olla mikä tahansa, mihin nimet on taltioitu
palvelimella.
NIMIbu=`cat /etc/hosts|grep -w $laite|grep -Eo 'labra-[r,s,w]{0,2}[0-9]{0,9}'`
#Käyttäjän valitessaan suoritettavaksi toiminnoksi “Telnet-vaihto-SSH-ja-AAA”
suoritetaan komento “cd /home/juho && ./konfiguroi-cisco.exp + muuttujat”
if [ $TASK == "Telnet-vaihto-SSH-ja-AAA" ]; then
    cd /home/juho && ./konfiguroi-cisco.exp $laite $USERNAME $PASSWORD
$ENABLEPASSWORD
#Vastaavasti mikäli valinta on SSH-keys niin suoritetaan komento joka johtaa
kyseiseen .exp -tiedostoon
elif [ $TASK == "SSH-keys" ]; then
    cd /home/juho && ./Cisco-ssh-avaimet.exp $laite $USERNAME $PASS-
WORD $ENABLEPASSWORD
#Vastaava tilanne, mikäli käyttäjä on valinnut varmuuskopioinnin
elif [ $TASK == "Backup" ]; then
    cd /home/juho && ./Backuppaus-cisco.exp $laite $USERNAME $PASS-
WORD $NIMIbu $PVMbu
fi
}
####  Ciscotoiminnot loppuu ####
#Dell toiminnot toimivat vastaavasti kuin Cisco
DellToiminnot ()
{
laite=$1
if [ $TASK == "Telnet-vaihto-SSH-ja-AAA" ]; then
```

```
    cd /home/juho && ./konfiguroi-dell.exp $laite $USERNAME $PASSWORD
$ENABLEPASSWORD
elif [ $TASK == "SSH-keys" ]; then
    cd /home/juho && ./dell-ssh-avaimet.exp $laite $USERNAME $PASSWORD
$ENABLEPASSWORD
elif [ $TASK == "Backup" ]; then
    cd /home/juho && ./dell-Backup.exp $laite $USERNAME $PASSWORD
$ENABLEPASSWORD
fi
}
### DellToiminnot Loppuu ###
#HP toiminnot toimivat myös vastaavasti
HPtoiminnot ()
{
laite=$1
if [ $TASK == "Telnet-vaihto-ssh-ja-AAA" ]; then
    cd /home/juho && ./konfiguroi-hp.exp $laite $USERNAME $PASSWORD
$ENABLEPASSWORD
elif [ $TASK == "SSH-keys" ]; then
    cd /home/juho && ./hp-ssh-avaimet.exp $laite $USERNAME $PASSWORD
$ENABLEPASSWORD
elif [ $TASK == "Backup" ]; then
    cd /home/juho && ./HP-Backup.exp $laite $USERNAME $PASSWORD $EN-
ABLEPASSWORD
fi
}
#Tehtävävalikkoa varten oleva aliohjelma
task_menu()
{
#Luodaan dialog –ikkunoita, joissa käyttäjä valitsee halutun toiminnon muuttu-
jaan TASK
dialog --clear  --backtitle "KELA - keskitetty tietoliikennelaitteiden hallinta" \
--title "[ TASK MENU ]" \
--menu "Valitse toiminto, jonka haluat suorittaa.\n
" 15 60 7 \
Telnet-vaihto-SSH-ja-AAA "SSH ja AAA konfiguraatiot" \
SSH-keys "SSH avainten vaihto" \
Backup "konfiguraatioiden backupit" \
VLAN "VLAN" \
Exit "Lopetus" 2>"${INPUT}"
menuitem=$(<"${INPUT}")
```

```
TASK=$(<"${INPUT}")
}

### TASK MENU LOPPUU ###
#Aliohjelma tunnistetietojen keräämistä varten
password()
{
#Määritellään muuttujalle data väliaikainen tiedosto, joka sitten voidaan myö-
hemmin poistaa.
data=$(tempfile 2>/dev/null)
trap "rm -f $data" 0 1 2 5 15
# Kysytään käyttäjänimeä
dialog --backtitle "Tunnistetietojen antaminen" \
 --title "Kayttajanimi" \
--clear \
--inputbox "Anna kayttajanimi:" 10 35 2> $data
#Otetaan väliaikaistiedostosta sinne kerätty merkkijono ja talletetaan se muut-
tujaan ”USERNAME”.
USERNAME=$(cat $data)
# Kysytään salasana
dialog --backtitle "Tunnistetietojen antaminen" \
--title "Salasana" \
--clear \
--insecure \
--passwordbox "Anna kayttajalle $USERNAME salasana:" 10 35 2> $data
ret=$?
# Päätös tehdään jälleen, ei pakollisia käytetty rakennusvaiheessa
case $ret in
  0)
    echo "Salasana on $(cat $data)";;
  1)
    echo "ESC valittu.";;
  255)
    [ -s $data ] &&  cat $data || echo "ESC pressed.";;
esac
#Otetaan väliaikaistiedostosta sinne kerätty merkkijono ja talletetaan se muut-
tujaan ”PASSWORD”.
PASSWORD=$(cat $data)
#Seuraavaksi vastaavasti halutaan enable-tilan salasana
dialog --backtitle "Tunnistetietojen antaminen" \
--title "Enable-salasana" \
```

```
--clear \
--insecure \
--passwordbox "Anna enable-tilan salasana:" 10 35 2> $data
ret=$?
# Päätös tehdään jälleen, ei pakollisia käytetty rakennusvaiheessa
case $ret in
  0)
    echo " ENA Salasana on $(cat $data)";;
  1)
    echo "ESC valittu.";;
  255)
    [ -s $data ] &&  cat $data || echo "ESC pressed.";;
esac
ENABLEPASSWORD=$(cat $data)
#Pyydetään käyttäjältä SNMP-kommunikaatiota varten merkkijonoa
dialog --backtitle "Tunnistetietojen antaminen" \
--title "SNMP Community String" \
--clear \
--insecure \
--passwordbox "Anna verkkolaitteen SNMP community string:" 10 35 2> $data
ret=$?
# Päätös tehdään jälleen, ei pakollisia käytetty rakennusvaiheessa
case $ret in
  0)
    echo "SNMP-kommunikointi on  $(cat $data)";;
  1)
    echo "ESC valittu.";;
  255)
    [ -s $data ] &&  cat $data || echo "ESC pressed.";;
esac
community=$(cat $data)
}
INPUT=/tmp/menu.sh.$$
OUTPUT=/tmp/output.sh.$$
# Kerätään tiedot ja tuhotaan ne
trap "rm $OUTPUT; rm $INPUT; exit" SIGHUP SIGINT SIGTERM
#Kutsutaan aliohjelmaa “password”, jolla aloitetaan koko ohjelman suorittami-
nen
password
#Tunnistetietojen keräyksen jälkeen aloitetaan “pääohjelmalla”, eli päävalikos-
sa, jossa käyttäjän on valittava laitevalmistaja
```

```
dialog --clear  --backtitle "KELA - keskitetty tietoliikennelaitteiden hallinta" \
--title "[ M A I N - M E N U ]" \
--menu "Tee valinta ylos/alas nuolinappaimia liikuttamalla. \n\
Paina halutun valmistajan kohdalla enter-painiketta. \
\n\
      \n          Valitse laitevalmistaja" 16 50 5 \
Cisco "CISCON laitteet" \
Dell "Dellin laitteet" \
HP "HPn laitteet" \
Exit "Lopetus" 2>"${INPUT}"
menuitem=$(<"${INPUT}")
# Päätös tehdään jälleen, ei pakollisia käytetty rakennusvaiheessa
case $menuitem in
        Cisco) VALM=CISCO;;
        Dell) VALM=DELL;;
        HP) VALM=HP;;
        Exit) echo "Bye"; break;;
esac

#Muistutetaan käyttäjää VAHTI-ohjeen mukaisesti siitä, että mikäli tämä aikoo
tehdä muutoksia laitteisiin, niin ottaa ensin varmuuskopiot laitteista

dialog --msgbox "Mikali olet tekemassa muutoksia niin\n      suorita ensiksi
backup!" \ 6 40
    clear
#Kutsutaan aliohjelmat " task_menu" ja sen jälkeen toiminnot
task_menu
toiminnot
#Alla olevat echot eivät ole oleellisia skriptin toiminnan kannalta, mutta on
suositeltavaa, että skriptiä kirjoittaessa tulostaa muuttujat lopussa, jotta voi-
daan havaita mikäli jokin muuttuja ei toimi oikein.
echo "USERNAME = $USERNAME"
echo "PASSWORD = $PASSWORD"
echo "TASK    = $TASK"
echo "VALM    = $VALM"
echo "SWnimet = $SWnimet"
echo "SWvalmistaja = $SWvalmistaja"
echo "Laite = $laite "
echo "Ena salasana = $ENABLEPASSWORD"
echo "SNMP community = $community"
#Lopuksi kerrotaan käyttäjälle, että toiminto on valmis ja mistä lokitiedot löyty-
vät mikäli halutaan varmistua, mitä on tullut tehtyä.
```

```
dialog  --msgbox "\n                    VALMIS! \n\nAjettujen konfiguraatoiden
lokitiedot loytyvat: /home/juho/ONT.log\n       Menu lokitiedot loytyvat
/home/juho/ONT-MENU.log \n\n                    Paina enter lopettaaksesi" \ 12 70
clear
#Etsitään vielä mahdollisia tietoja, niiden ilmaantuessa poistetaan ne.
[ -f $OUTPUT ] && rm $OUTPUT
[ -f $INPUT ] && rm $INPUT
```

Liite 6. Cisco-konfiguraatio.exp

```
#!/usr/bin/expect -f
#Luodaan tarvittavat muuttujat yhteyttä varten argumentteinä
    #Aikakatkaisu
    set timeout 20
    #IP-osoite, jonka arvo on ensimmäinen käytettävä parametri itse
ajokomennon jälkeen esim. ./Cisco-konfiguraatio 10.10.10.10
    set IPaddress [lindex $argv 0]
   #Käyttäjänimi, jonka avulla kirjaudutaan laitteisiin, toinen parametri
    set UserName [lindex $argv 1]
    #Salasana, jota käyttäjänimi käyttää kirjautumiseen, kolmas parametri
    set PassWord [lindex $argv 2]
   #Enable-tilan salasana, jonka avulla voidaan siirtyä enable tilaan, neljäs pa-
rametri
    set enable [lindex $argv 3]
  #määritetään tiedosto, johon lokitetaan tiedoston ajon aloitus aika
    log_file -a /home/juho/ONT.log
#Aloitetaan konfigurointi, josta tehdään ilmoitus lokitiedostoon, että istunto al-
koi osoitteeseen tiettyyn aikaan
    send_log "### /TELNET-SESSIO-ALKOI-OSOITTEESEEN/ IP: $IPaddress @
[exec date] ###\r"
   #Muodostetaan yhteys muuttujaan IPaddress
   spawn telnet $IPaddress
 #Aloitetaan konfigurointi kirjautumalla laitteeseen ja siitä eteenpäin  odote-
taan  (expect) tiettyä merkkijonoa johon vastataan lähettämällä (send) tietty
merkkijono
   expect "*"
   send "$UserName\n"
   expect "*"
   send "$PassWord\r"
   expect "*>"
```

```
    send "ena\n"
    expect "*"
    send "$enable\n"
    expect "*"
    send "configure terminal\n"
    expect "*fig)#"
    send "crypto key generate rsa\n"
    expect "*"
  send "1024\n"
  expect "*fig)#"
  send "no ip domain lookup\n"
  expect "*fig)#"
  send "ip ssh version 2\n"
 expect "*fig)#"
 send "ip scp server enable\n"
 expect "*fig)#"
 send "line vty 0 15\n"
 expect "*fig-line)#"
send "transport input ssh\n"
expect "*fig-line)#"
send "exit\n"
expect "*fig)#"
send "aaa new-model\n"
expect "*fig)#"
send "aaa authentication login default group tacacs+\n"
expect "*fig)#"
send "aaa authentication login console local\n"
expect "*fig)#"
send "aaa authorization exec default group tacacs+\n"
expect "*fig)#"
send "aaa authorization exec console local\n"
expect "*fig)#"
send "aaa accounting commands 15 default start-stop group tacacs+\n"
expect "*fig)#"
send "aaa accounting system default start-stop group tacacs+\n"
expect "*fig)#"
send "tacacs-server host 172.16.40.20 key labra\n"
expect "*fig)#"
send "ip tacacs source interface fastethernet0/0.10\n"
expect "*fig)#"
```

```
    send "access-list 101 permit tcp host 172.16.40.10 172.16.10.0 0.0.0.255 eq 22
    log\n"
    expect "*fig)#"
   send "access-list 101 permit tcp host 172.16.40.30 172.16.10.0 0.0.0.255 eq 22
     log\n”
  expect "*fig)#"
    send "access-list 101 permit udp host 172.16.40.10 172.16.10.0 0.0.0.255 eq
    snmp log\n"
    expect "*fig)#"
send "line vty 0 15\n"
expect "*
send "access-class 101 in\n"
expect “*”
send “exit\n”
send "banner login CCHyvaa Paivaa!CC\n"
expect "*fig)#"
send "line con 0\n"
expect "*ig-line)#"
send "login authentication console\n"
expect "*ig-line)#"
send "exit\n"
expect "*fig)#"
send "clock timezone EET 2\n"
expect "*fig)#"
send "ntp server 172.16.40.10\n"
expect "*fig)#"
send "end\n"
expect "*#"
send ”wr mem\n”
send "end\n"
expect "*#"
send "logout\n"
expect eof
send_log "\r### /END-TELNET-SESSION/ IP: $IPaddress @ [exec date] ###\r"
exit
```

Liite 7. Autobu.sh & Backuppaus-cisco.exp

```
#!/bin/bash –x
#Määritetään varmuuskopiointia varten käyttäjätiedot, SNMP-kommunikointia varten merkkijon, aikaleima, SySoidit ja Laitteet tietystä tiedostosta
Kayttaja=Backuppaaja
Passwd=ASGfc2g_sadYHRhe
Community=labra
PVM=`date +%d.%m.%y_Ajassa_%H:%M`
HPJONO=iso.3.6.1.4.1.11
DELLJONO=iso.3.6.1.4.1.674
CISCOJONO=iso.3.6.1.4.1.9
SWlaitteet=`grep -Eo '172\.16\.10\.[0-9]{1,3}' /etc/hosts`
#Aliohjelma Cisco, joka vertaa diff-komennolla uutta ja vanhaa varmuuskopiota, mikäli rivieroja on enemmän kuin 0 niin siirretään vanha tiedosto eri kansioon, muuten poistetaan uusi. Sama toistetaan Dell- ja HP –aliohjelmissa.
cisco()
{
laite=$1
nimi=`cat /etc/hosts|grep -w $laite|grep -Eo 'labra-[r,s,w]{0,2}[0-9]{0,9}'`
        cd /home/juho/ && ./Backuppaus-cisco.exp $laite $Kayttaja $Passwd $nimi $PVM
buc1=`cd /home/juho/config-backupt/ && ls |grep Cisco-$nimi.cfg.$PVM`
buc2=`cd /home/juho/config-backupt/ && ls |grep Cisco-$nimi.cfg |grep -v $PVM`
vertaus=`diff --brief /home/juho/config-backupt/$buc1 /home/juho/config-backupt/$buc2 |wc -l`
        if [ $vertaus -gt 0 ]; then
        mv /home/juho/config-backupt/$buc2 /home/juho/config-backupt/vanhat
        else
        rm /home/juho/config-backupt/$buc1
fi
}
dell()
{
laite=$1
nimi=`cat /etc/hosts|grep -w $laite|grep -Eo 'labra-[r,s,w]{0,2}[0-9]{0,9}'`
        cd /home/juho/ && ./Backuppaus-dell.exp $laite $Kayttaja $Passwd $nimi $PVM
bud1=`cd /home/juho/config-backupt/ && ls |grep Dell-$nimi.cfg.$PVM`
```

```
bud2=`cd /home/juho/config-backupt/ && ls |grep Dell-$nimi.cfg |grep -v $PVM`
vertaus=`diff --brief /home/juho/config-backupt/$bucd /home/juho/config-backupt/$bucd |wc -l`
        if [ $vertaus -gt 0 ]; then
        mv /home/juho/config-backupt/$bud2 /home/juho/config-backupt/vanhat
        else
        rm /home/juho/config-backupt/$bud1
}
hp()
{
laite=$1
nimi=`cat /etc/hosts|grep -w $laite|grep -Eo 'labra-[r,s,w]{0,2}[0-9]{0,9}'`
        cd /home/juho/ && ./Backuppaus-HP.exp $laite $Kayttaja $Passwd $nimi $PVM
buh1=`cd /home/juho/config-backupt/ && ls |grep HP-$nimi.cfg.$PVM`
buh2=`cd /home/juho/config-backupt/ && ls |grep HP-$nimi.cfg |grep -v $PVM`
vertaus=`diff --brief /home/juho/config-backupt/$buh1 /home/juho/config-backupt/$buch |wc -l`
        if [ $vertaus -gt 0 ]; then
        mv /home/juho/config-backupt/$buh2 /home/juho/config-backupt/vanhat
        else
        rm /home/juho/config-backupt/$buh1
}

#Tehdään snmp-kyselyä aiemmin kerätyille laitteille ja määritellään muuttujat laitevalmistajien mukaisesti ja tehdään säännöt, että jos löytyy enemmän kuin 0 niin suoritetaan varmuuskopiointi prosessi kyseiselle laitevalmistajalle.

for i in $SWlaitteet
do
        VALM=`snmpwalk -c $Community -v2c $i 1.3.6.1.2.1.1.2`
        CISCO=`echo $VALM|grep $CISCOJONO|wc -l`
        DELL=`echo $VALM |grep $DELLJONO|wc –l`
        HP=`echo $VALM |grep $HPJONO |wc -l`
        if [ $CISCO -gt 0 ]; then
                        cisco $i
        elif [ $DELL –gt 0]; then
                        dell $i
        elif [ $HP –gt 0 ]; then
```

```
                    hp $i
fi
done
```

#---Backuppaus-cisco.exp--- alkaa#

```
#Määritetään argumentit, joita käytetään varmuuskopioinnissa ja määritetään lokitiedosto. Komennetaan SCP:llä ilman avaimen tarkistusta system:running-config-tiedoston haku. Ciscolla voi varmistaa #dir system:-komenolla, että running-config löytyy varmasti oikeasta paikasta. loppuun vielä lokitetaan, että varmuuskopiointi on loppunut.
#!/usr/bin/expect -f
set osoite [lindex $argv 0]
set user [lindex $argv 1]
set passwd [lindex $argv 2]
set NIMI [lindex $argv 3]
set PVM [lindex $argv 4]
log_file -a /home/juho/BU.log
send_log "### /AKTIIVILAITTEEN $NIMI VARMUUSKOPITOINTI ALKOI / IP: $osoite @ $PVM###"
spawn scp -o StrictHostKeyChecking=no $user@$osoite:system:running-config /home/juho/config-backupt/Cisco-$NIMI.cfg.$PVM
expect "*as*"
send "$passwd\r"
expect eof
send_log "\r### /AKTIIVILLAITTEEN $NIMI VARMUUSKOPIOINTI LOPPUI / IP: $osoite @ $PVM ###\r"
exit
```

Liite 8. VAHTI sisäverkko-ohjeen viitteet

Tunnistautumisen tarkituslista	Korotettu taso
15.2 Käyttäjän tunnistautumisessa käytetään henkilökohtaisia tunnuksia. Tämä koskee myös ylläpitotunnuksia.	Pakollinen vaatimus
15.3 Etäyhteyksien muodostamiseen ei käytetä pelkkää käyttäjätunnus/salasanaparia	Pakollinen vaatimus
15.7 Tunnus lukkiutuu, mikäli järjestelmään yritetään epäonnistuneesti liian monta kertaa	Pakollinen vaatimus
15.12 Epäonnistuneet kirjautumisyritykset sekä muut valtuuksien puutteeseen kariutuvat toimenpideyritykset kirjataan	Pakollinen vaatimus
15.13 Kaikkien verkkotuotteiden ja muiden valmisohjelmistojen oletustunnusten salasanat on vaihdettu oletusarvosta tai oletustunnus on poistettu	Pakollinen vaatimus
15.17 Tunnistautumisessa käytetään menetelmiä, joissa tunnistautumiseen käytettävät tiedot, kuten käyttäjätunnukset ja salasanat eivät kulje verkon yli salaamattomana	Pakollinen vaatimus

Hallinnan/Valvonnan tarkistuslista	Korotettu taso
16.1 Lokit tallennetaan keskitetylle lokipalvelimelle	Vahva suositus
16.2 Laitteiden lokiasetukset on määritetty sellaisiksi, että lokeista saadaan tietoa verkon toiminnasta	Pakollinen vaatimus
16.4 Hallintaliikenne salataan riittävällä tasolla, jotta ulkopuolinen henkilö ei pysty seuraamaan tehtäviä muutoksia eikä tunnistautumaan hallintakäyttäjänä	Pakollinen vaatimus
16.8 Lokit suojataan muutoksilta	Vahva suositus
16.15 Lokeista pystytään jälkikäteen selvittämään mitä hallintatoimenpiteitä verkkolaitteille on tehty, milloin ja kenen toimesta (Audit trail)	Vahva suositus
16.20 Verkon hallinta ja valvonta tehdään laitteilla, jotka on fyysisesti erotettu muista työasemista	Vahva suositus
16.24 Ylläpitopääsy verkon laitteille on rajoitettu verkon valvonta- ja hallinta-työasemille. Rajaus on toteutettu verkon sisällä sekä verkon ulkopuolella etäylläpidossa	Pakollinen vaatimus
16.25 Valvontaan käytetyillä tunnuksilla on vain lukuoikeus verkon lokitietoihin	vahva suositus

Jatkuvuussuunnittelun tarkistuslista	Korotettu taso
17.7 Varmuuskopioilta palauttamista testataan säännöllisesti	Vahva suositus
17.25 Varmuuskopioinnin onnistumista valvotaan systemaattisesti	Vahva suositus
17.26 Varmuuskopiot otetaan myös ennen olennaisia muutoksia ja niiden jälkeen	Vahva suositus

Liite 9. Cisco ACS appliance konfiguraatiot (olennaiset)

```
hostname cisco-acs
ip domain-name Labra.local
interface GigabitEthernet 0
 ip address 172.16.40.20 255.255.255.0
ipv6 address autoconfig
ip name-server 172.16.40.10
ip default-gateway 172.16.40.1
clock timezone UTC
ntp server 172.16.40.10
username admin password hash $1$NsqLkTO7$w5hyNkOt42.tpvxsg7PPl/ role
admin
service sshd
logging 172.16.40.10
logging loglevel 6
icmp echo on
```

Liite 10. Labra-R1 konfiguraatiot (olennaiset)

```
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
hostname Labra-R1
enable secret 5 $1$h025$5btW3WqKuDs/rofR6Mlcq1
enable password cisco
aaa new-model
aaa authentication login default group tacacs+
aaa authentication login console local
aaa authorization exec default group tacacs+
aaa authorization exec console local
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
aaa session-id common
clock timezone EET 2
no ip domain lookup
ip domain name labra.local
ip ssh version 2
```

```
ip scp server enable
username cisco secret 5 $1$qO4Y$wZLErbAsvLQ7l/VuDp4IK.
interface Loopback0
 description internet-kuvaaja
 ip address 90.90.90.90 255.255.255.255
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/0.10
 description Hallinta GW
 encapsulation dot1Q 10
 ip address 172.16.10.1 255.255.255.0
!
interface FastEthernet0/0.20
 description Tuotanto GW
 encapsulation dot1Q 20
 ip address 172.16.20.1 255.255.255.0
!
interface FastEthernet0/0.30
 description VerkkoAdmins GW
 encapsulation dot1Q 30
 ip address 172.16.30.1 255.255.255.0
!
interface FastEthernet0/0.40
 description Palvelimet GW
 encapsulation dot1Q 40
 ip address 172.16.40.1 255.255.255.0
!
interface FastEthernet0/0.50
 description Vieras GW
 encapsulation dot1Q 50
 ip address 172.16.50.1 255.255.255.0
 no snmp trap link-status
interface FastEthernet0/0.99
 description Accounting Test
!
ip tacacs source-interface FastEthernet0/0.10
!
snmp-server community labra RW
snmp-server host 172.16.10.11 version 2c labra
snmp-server tftp-server-list 10
!
tacacs-server host 172.16.40.20 key labra
tacacs-server directed-request
!
```

```
line con 0
 login authentication console
line vty 0 4
 session-timeout 15
 access-class 101 in
 transport input ssh
line vty 5 15
 access-class 101 in
 transport input ssh
line vty 16 55
 transport input telnet
!
ntp server 172.16.40.10
end
```

Liite 11. Labra-sw1 konfiguraatiot (olennaiset)

```
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname Labra-sw1
enable password cisco
username cisco password 0 cisco
aaa new-model
!
aaa authentication login default group tacacs+
aaa authentication login console local
aaa authorization exec default group tacacs+
aaa authorization exec console local
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
!
aaa session-id common
clock timezone EET 2
ip routing
no ip domain-lookup
ip domain-name labra.local
!
vlan 10
 name hallinta
!
vlan 20
```

```
 name tuotanto
!
vlan 30
 name VerkkoAdmins
!
vlan 40
 name Palvelimet
!
vlan 50
 name Vieras
!
ip ssh version 2
ip scp server enable
interface GigabitEthernet1/0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet1/0/2
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet1/0/3
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet1/0/17
 switchport access vlan 40
 switchport mode access
!
interface GigabitEthernet1/0/18
 switchport access vlan 50
 switchport mode access
!
interface GigabitEthernet1/0/48
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface Vlan10
 ip address 172.16.10.10 255.255.255.0
!
ip classless
ip route 0.0.0.0 0.0.0.0 172.16.10.1
snmp-server community labra RO
tacacs-server host 172.16.40.20 key labra
tacacs-server directed-request
!
line con 0
```

```
 logging synchronous
 login authentication console
 escape-character 3
line vty 0 4
 access-class 101 in
 logging synchronous
 transport input ssh
 escape-character 3
line vty 5 15
 access-class 101 in
 transport input ssh
!
ntp server 172.16.40.10
end
```

Liite 12. Labra-sw2 konfiguraatiot (olennaiset)

```
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname Labra-sw2
enable password cisco
!
username cisco password 0 cisco
!
aaa new-model
!
aaa authentication login default group tacacs+
aaa authentication login console local
aaa authorization exec default group tacacs+
aaa authorization exec console local
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
!
aaa session-id common
clock timezone EET 2
!
no ip domain-lookup
ip domain-name labra.local
!
vlan 10
 name hallinta
!
vlan 20
```

```
 name tuotanto
!
vlan 30
 name VerkkoAdmins
!
vlan 40
 name Palvelimet
!
vlan 50
 name Vieras
!
ip ssh version 2
ip scp server enable
!
interface GigabitEthernet0/1
 switchport access vlan 40
 switchport mode access
!
interface GigabitEthernet0/11
 switchport access vlan 40
 switchport mode access
!
interface GigabitEthernet0/20
 switchport access vlan 40
 switchport mode trunk
!
interface Vlan10
 ip address 172.16.10.20 255.255.255.0
 no ip route-cache
snmp-server community labra RO
tacacs-server host 172.16.40.20 key labra
no tacacs-server directed-request
!
line con 0
 authorization exec console
 login authentication console
line vty 0 4
 access-class 101 in
 transport input ssh
line vty 5 15
 access-class 101 in
 transport input ssh
!
ntp server 172.16.40.10
end
```

Liite 13. Labra-sw3 konfiguraatiot (olennaiset)

```
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname Larba-sw3
enable password cisco
!
username cisco password 0 cisco
!
aaa new-model
!
aaa authentication login default group tacacs+
aaa authentication login console local
aaa authorization exec default group tacacs+
aaa authorization exec console local
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
!
aaa session-id common
clock timezone EET 2
!
no ip domain-lookup
ip domain-name labra.local
!
vlan 10
 name hallinta
!
vlan 20
 name tuotanto
!
vlan 30
 name VerkkoAdmins
!
vlan 40
 name Palvelimet
!
vlan 50
 name Vieras
!
ip ssh version 2
ip scp server enable
!
```

```
interface GigabitEthernet0/3
 switchport mode trunk
!
interface GigabitEthernet0/12
 switchport access vlan 40
 switchport mode access
!
interface GigabitEthernet0/13
 switchport access vlan 30
 switchport mode access
!
interface Vlan10
 ip address 172.16.10.30 255.255.255.0
 no ip route-cache
snmp-server community labra RO
tacacs-server host 172.16.40.20 key labra
no tacacs-server directed-request
!
line con 0
 authorization exec console
 login authentication console
line vty 0 4
 access-class 101 in
 transport input ssh
line vty 5 15
 access-class 101 in
 transport input ssh
!
ntp server 172.16.40.10
end
```

Liite 14. Labra-sw4 konfiguraatiot (olennaiset)

```
configure
vlan database
vlan  10,20,30,40,50
exit
hostname "Labra-sw4"
no ip domain-lookup
ip domain-name labra.local
interface vlan 10
routing
ip address  172.16.10.40  255.255.255.0
exit
ip routing
```

ip route 0.0.0.0 0.0.0.0 172.16.10.1
username "cisco" password 07982c55db2b9985d3391f02e639db9c level 1 encrypted
aaa authentication login "TACACS" tacacs
aaa authentication login "CONSOLE" none
aaa authentication enable "TACACS" tacacs
aaa authentication enable "CONSOLE" none
tacacs-server host 172.16.40.20
key "labra"
exit
line console
login authentication CONSOLE
enable authentication CONSOLE
exit
line ssh
login authentication TACACS
enable authentication CONSOLE
exit
ip ssh server
!Management ACAL
management access-list "DENY"
deny service telnet priority 1
deny service http priority 2
deny service https priority 3
permit ip-source 172.16.0.0 mask 255.255.0.0 priority 4
permit ip-source 172.16.10.100 mask 255.255.255.255 vlan 10 service ssh priority 5
permit ip-source 172.16.0.0 mask 255.255.0.0 service ssh priority 6
permit ip-source 172.16.0.0 mask 255.255.0.0 service telnet priority 7
exit
!
interface ethernet 1/g1
switchport mode trunk
switchport trunk allowed vlan add 10,20,30,40,50
switchport trunk allowed vlan remove 1
exit
!
interface ethernet 1/g2
no negotiation
switchport access vlan 10
exit
snmp-server community labra ro
snmp-server host 172.16.40.10 labra informs
snmp-server host 172.16.40.10 labra traps v2
!
exit

Liite 15. AD-palvelimen konfiguraatio Excel-taulukko

Alla olevassa kuviossa on esitetty Excel-taulukosta kuvankaappaus. Kuviossa on näkyvissä kaikki oleelliset kentät, joita muokkaamalla syötetty sarakkeen ”K” komento muokkautuu sopivaksi.

	A	B	C	D	E	F	G	H	I	J	K
1		UusiOu	DC-osa1	DC-osa2	Ryhmä	Security group	Desc	Käyttäjän etunimi / Koneen nimi	Käyttäjän sukunimi	Käyttäjän OU	Komento
2	Dsadd (ou)	ACS	Labra	local							dsadd ou ou=ACS,dc=Labra,dc=local
3	Dsadd (group)	ACS	Labra	local	ACS-Hallinta	yes	ACS-Hallintaryhma				dsadd group cn=ACS-Hallinta,ou=ACS,dc=Labra,dc=local -secgrp yes -desc ACS-Hallintaryhma
4	Dsmod (Kone)	ACS	Labra	local	ACS-Hallinta		ACS-palvelin	ACS-palvelin1			dsadd computer cn=ACS-palvelin1,cn=ACS-Hallinta,dc=Labra,dc=local -desc ACS-palvelin
5	Dsmod (käyttäjä)	ACS	Labra	local	ACS-Hallinta			Matti	Meikalainen	Users	dsmod group "cn=ACS-Hallinta,ou=ACS,dc=Labra,dc=local" addmbr "cn=Matti Meikalainen,cn=Users,dc=Labra,dc=local"
6	Dsmod (käyttäjä)	ACS	Labra	local	ACS-Hallinta			Teppo	Testaaja	Users	dsmod group "cn=ACS-Hallinta,ou=ACS,dc=Labra,dc=local" addmbr "cn=Teppo Testaaja,cn=Users,dc=Labra,dc=local"
7	Dsmod (käyttäjä)	ACS	Labra	local	ACS-Hallinta					Users	dsmod group "cn=ACS-Hallinta,ou=ACS,dc=Labra,dc=local" addmbr "cn= ,cn=Users,dc=Labra,dc=local"
8	Dsmod (käyttäjä)	ACS	Labra	local	ACS-Hallinta					Users	dsmod group "cn=ACS-Hallinta,ou=ACS,dc=Labra,dc=local" addmbr "cn= ,cn=Users,dc=Labra,dc=local"
9	Dsmod (käyttäjä)	ACS	Labra	local	ACS-Hallinta			Juho	Myllys	Users	dsmod group "cn=ACS-Hallinta,ou=ACS,dc=Labra,dc=local" addmbr "cn=Juho Myllys,cn=Users,dc=Labra,dc=local"

Excel-taulukko AD-palvelimelle tietojen lisäämistä varten

Ensimmäisellä rivillä määritellään tiedot uutta OU:ta varten eli toimialueen tiedot ja OU:n nimi ovat tarvittavia tietoja. K-sarakkeen komento on seuraavanlainen:

=KETJUTA("dsadd ou ou=";B2;",dc=";C2;",dc=";D2;)

Seuraava rivi on ryhmän luontia varten. Tällä rivillä määritellään ryhmälle nimi, toimialue, OU, security group sekä kuvaus. K-sarakkeen komento on seuraavanlainen:

=KETJUTA("dsadd group cn=";E3;",ou=";B3;",dc=";C3;",dc=";D3;" -secgrp ";F3;" -desc ";G3;)

Seuraavalla rivillä luodaan ACS-palvelinta varten kone, joka liitetään edellä luotuun ryhmään. K-sarakkeen komento on seuraavanlainen:

=KETJUTA("dsadd computer cn=";H4;",cn=";E4;",dc=";C4;",dc=";D4;" -desc ";G4;"")

Seuraavalla rivillä määritetään käyttäjää varten tiedot, tarkemmin sanottuna muokataan aikaisemmin luotua ryhmää liittämällä siihen olemassa olevia käyttäjiä. Tietoihin tulee antaa OU:n nimi, ryhmän nimi, toimialue, etu- ja sukunimi. K-sarakkeen komento on seuraavanlainen:

=KETJUTA("dsmod group ""cn=";E4;",ou=";B4;",dc=";C4;",dc=";D4;""" -addmbr ""cn=";H4;" ";I4;",cn=";J4;",dc=";C4;",dc=";D4;""")

Toiminnaltaan itse Excel-tiedosto ei tee mitään. K-sarakkeesta on ”maalattava” kohdat, jotka halutaan konfiguroida AD-palvelimelle, kopioida ne ja liittää AD-palvelimella komentoriville, jota suoritetaan järjestelmävalvojan oikeuksin.

Kyseisen Excel-tiedoston avulla voidaan helposti luoda myös valvonta ryhmä AD-palvelimelle muuttamalla ainoastaan ryhmän nimeksi esimerkiksi *ACS-valvonta* ja *Dsmod (käyttäjä)*-riveille lisäämällä henkilöiden nimet, jotka ovat valtuutettuja valvomaan laitteita. Kyseinen tiedosto on yleispätevä ja sitä voidaan toki hyödyntää muihinkin lisäämisprosesseihin kuin ainoastaan ACS-palvelimeen liittyviin.

Liite 16. Raportoinnin osa-alueet

Ensimmäisenä on pääsivun konfiguraatiotiedosto, sivu on siis se, joka näkyy käyttäjälle.

```
#!/bin/sh
#CGI -tiedostojen tulee olla /usr/lib/cgi-bin/ kansiossa
echo "Content-type: text/html\n"
echo ' '
/bin/cat << EOM
<HTML>
<HEAD><TITLE>ACS RAPORTIT </TITLE>
</HEAD>
<frameset cols="25%,75%">
<frame name="ACS-palvelimen raportit:" SRC=Raportit.cgi>
<frame name="Viikon autentikonnit" >
<BODY>
</HTML>
EOM
```

Seuraavana on sivu, jossa määritellään itse raportit ja niiden Google-URL:t

```
#!/bin/sh
echo "Content-type: text/html\n"
echo ' '
```

```
/bin/cat << EOM
<BODY>
<p>ACS RAPORTIT:</p>
<ACS-palvelimen raportit:>
<li><a
href="https://chart.googleapis.com/chart?cht=bvg&chs=440x340&chd=t:20,35,10,10,5,10,15|30,44,25,5,7,36,11&chxr=1,0,50&chds=0,50&chco=389ced,FF0000&chbh=15,0,20&chxt=x,y&chxl=0:|Ma|Ti|Ke|To|Pe|La|Su&chdl=AuthOK|AuthFail&chg=0,5,5,5" TARGET="Viikon autentikonnit"> Autentikaatioraportti viikolta 11</a>
<li><a
href="https://chart.googleapis.com/chart?cht=bvg&chs=440x340&chd=t:13,15,8,4,3,12,19|5,12,2,9,1,12,11&chxr=1,0,50&chds=0,50&chco=389ced,FF0000&chbh=15,0,20&chxt=x,y&chxl=0:|Ma|Ti|Ke|To|Pe|La|Su&chdl=AuthOK|AuthFail&chg=0,5,5,5" TARGET="Viikon autentikonnit">Autentikaatioraportti viikolta 12 </a>
</BODY>
</HTML>
```

Viimeisenä osana on raporttien viikoittaiseen lisäämiseen tarkoitettu skripti. (Joka on ajastettu *crontab*-ominaisuudella)

```
#!/bin/bash
#määritellään muuttujat
PVM=`date +%D_%W`
Raportit=`/home/juho/raporttitiedot.txt`
VKOlkm=`date +%W`
#Filulla voi olla oikeuksia melko paljon poiston takia. Kyseinen #Skripti ajastetaan crontabiin 10min sen jälkeen kun acs on tehnyt #oman lokituksensa
#Raportti luodaan joka sunnuntain esim. 23.55. ACS -palvelimen tuottamat lokitapahtumat eivät sisällä viikonpäiviä, joten luodaan tieto niistä käsin.
su=`date +%Y-%m-%d`
la=`date --date '- 1 days' +%Y-%m-%d`
pe=`date --date '- 2 days' +%Y-%m-%d`
to=`date --date '- 3 days' +%Y-%m-%d`
ke=`date --date '- 4 days' +%Y-%m-%d`
ti=`date --date '- 5 days' +%Y-%m-%d`
ma=`date --date '- 6 days' +%Y-%m-%d`
#Alla olevissa muuttujissa huomioitava, että kyseiset keräävät tietoa SysLog –lokitiedoista, joten kyseisen lokitiedoston oikeudet muutettava, että niitä voidaan lukea ilman sudo-oikeuksia.
#Onnistuneet päiväkohtaiset autentikaatiot
maok=`cat /var/log/acs-loki.log |grep $ma |grep success |wc -l`
```

```
tiok=`cat /var/log/acs-loki.log |grep $ti |grep success |wc -l`
keok=`cat /var/log/acs-loki.log |grep $ke |grep success |wc -l`
took=`cat /var/log/acs-loki.log |grep $to |grep success |wc -l`
peok=`cat /var/log/acs-loki.log |grep $pe |grep success |wc -l`
laok=`cat /var/log/acs-loki.log |grep $la |grep success |wc -l`
suok=`cat /var/log/acs-loki.log |grep $su |grep success |wc -l`
#Epäonnistuneet päiväkohtaiset autentikaatiot
maei=`cat /var/log/acs-loki.log |grep $ma |grep fail |wc -l`
tiei=`cat /var/log/acs-loki.log |grep $ti |grep fail |wc -l`
keei=`cat /var/log/acs-loki.log |grep $ke |grep fail |wc -l`
toei=`cat /var/log/acs-loki.log |grep $to |grep fail |wc -l`
peei=`cat /var/log/acs-loki.log |grep $pe |grep fail |wc -l`
laei=`cat /var/log/acs-loki.log |grep $la |grep fail |wc -l`
suei=`cat /var/log/acs-loki.log |grep $su |grep fail |wc -l`

#Määritellään muuttuja Raportti, joka on käytännössä www-osoite, jonka ko-
pioimalla selaimeen päästään suoraan tarkastelemaan kaavioita

Raportti="<li><a
href=\"https://chart.googleapis.com/chart?cht=bvg&chs=440x340&chd=t:$ma
ok,$tiok,$keok,$took,$peok,$laok,$suok|$maei,$tiei,$keei,$toei,$peei,$laei,$su
ei&chxr=1,0,50&chds=0,50&chco=389ced,FF0000&chbh=15,0,20&chxt=x,y&chx
l=0:|Ma|Ti|Ke|To|Pe|La|Su&chdl=AuthOK|AuthFail&chg=90,5,5,5\" TAR-
GET=\"Viikon autentikoinnit\">Autentikaatio Raportti viikolta $VKOlkm
</a>"sivupolku=/usr/lib/cgi-bin/ONT-raportit.cgi

Valitiedosto=muutos1.$$
#"heitetään" raportti urli cgi-bin/ONT-raportit.cgi –tiedostoon alimman <a
href= -kohdan alle
awk -v l="$Raportti" '/<li><a href=/{x=NR}
{a[NR]=$0;}END[{for(i=1;<=NR;i++){fi(i==x+1)print l; print a[i];}}' $sivupolku
>$Valitiedosto
cp $Valitiedosto $sivupolku
rm -f $Valitiedosto
```

Liite 17. VAHTI sisäverkko-ohjeen osa-alueet

Tunnistautumisen tarkistulista	Ratkaisu
15.2 - OK	AD-palvelimella omat tunnukset
15.3 - OK	OK, mikäli käytössä hallinta-asema, johon kirjaudutaan omalla avaimella
15.7 - OK	GPO lukittaa tunnuksen kolmen epäonnistuneen kirjautumisen jälkeen
15.12 - OK	ACS-palvelimelle jää kaikista kirjautumisyrityksistä jälki ja ne voidaan halutessa lokittaa SysLog-palvelimelle
15.13 - OK	ACS-palvelin ainut, jossa oli oletustunnus, joka pakotettiin vaihtamaan
15.17 - OK	TACACS+ salaa koko istunnon näiltä osin

Hallinnan/Valvonnan tarkistuslista	
16.1 - OK	OK - Käytettiin erillistä SysLog -palvelinta ja ACS lokitti omansa
16.2 - OK	OK, saadaan kattavaa tietoa laitteiden toiminnasta
16.4 - OK	SSH-yhteys otettiin käyttöön
16.8 - OK	Lokeja voi muokata vain SUDO-oikeuksin varustetut henkilöt
16.15 - OK	Audit trail saatiin käyttöön Ciscon ja HP:n laitteissa, eli osittain OK
16.20 - OK	Työssä käytettiin erillistä hallinta-asemaa
16.24 - OK	Rajaus tehtiin Pääsylistoilla
16.25 - OK	Valvontatunnukset alempi privilege-taso ja ACS:llä valvonta rooli käytössä

Jatkuvuussuunnittelun tarkistulista	
17.7 - EI	Ei pystytty tekemään todennetusti, mutta testattiin ja toimi
17.25 - OK	Valvotaan, lokitetaan autentikaatiot WWW-sivulle ja ACS-palvelimelta voidaan käsin valvoa
17.26 - OK	Luotiin käyttöliittymään muistutus, jotta kyseinen asia oikeasti muistetaan tehdä, ja varmuuskopiot otetaan joka päivä

KANSANELÄKELAITOS
IT-osasto
Teknologiaryhmä/Integraatiotiimi
Juha Lappalainen

7.8.2013

Liite 18 Toimeksiantajan palaute

Lausuntopyyntö

Keskitetyn käyttäjähallinnan suunnittelu ja toteuttaminen Kansaneläkelaitoksen aktiivilaitteisiin

Tuotannossa saavutettavat edut

Keskitetynkäyttäjähallinnan kehittämisen idea syntyi käytännön tarpeesta, jonka tarkoituksena oli lisätä tietoverkon tietoturvaa aktiivilaitteiden kohdalla. Keskitetyn käyttäjähallinnan lisäksi pyrittiin lisäämään tietoturvaa muillakin keinoilla kuten, salatut hallintayhteydet ja automaattinen varmuuskopiointi.

Opinnäytetyöllä tullaan saavuttamaan käyttöönoton yhteydessä merkittäviä etuja tietoverkon näkökulmasta niin tietoturvallisuuden, hallittavuuden ja ylläpidon osalta.

Työllä saavutettiin seuraavia hyötyjä:

- Keskitettykäyttäjähallinta tietoverkon aktiivilaitteille
- Hallintayhteyksien tietoturvan lisäys
- Automaattinen varmuuskopiointi verkon aktiivilaitteille, joka ottaa huomioon konfiguraatiotiedostojen muuttuvuuden, eli ns. turhia tiedostoja ei säilötä.
- Aktiivilaitteiden hallintaroolien määrittäminen säädettiin automaattiseksi
- Verkkovikojen vianselvitys helpottui, sillä käyttöön saatiin ’Audit Trail’ – toiminne.

Käytännön hyötyjen lisäksi työllä saavutettiin etuja myös kustannuksien kohdalla:

- Varmuuskopiointi suoritettiin käsin ohjelmoimalla ja se asetettiin automaattiseksi, jonka seurauksena ei tarvinnut hankkia ulkopuolista tuotetta tai vaihtoehtoisesti työntekijöiden ei tarvitse tehdä varmuuskopiointia enää käsin. Aktiivilaitteita on useita, joten jokaisen laitteen varmuuskopiointi veisi viikkotasolla n. 2 tuntia (kirjautuminen + kopiointi).

Vuodessa:
52(viikot)*5(arkipäivät)*2(työmäärä/vko)*50€(Tuntipalkka-arvio) = 26.000 €

- Protokollan/Tuotteen valinnassa ei ollut tarvetta käyttää ulkopuolista konsulttia, jonka seurauksena saavutettiin säästöjä. 100€/h ja noin 2 viikon työ selvityksineen, kuten protokollien ja tuotteiden ominaisuudet, kirjallisien raporttien kanssa, eli 100*2*37,5h = 7500€

- Aktiivilaitteiden konfiguraatioiden suunnittelu ja testaaminen aktiivilaitteisiin säästi vakituisten (2hlö) toimihenkilöiden työaikaa noin viikon työtunnit. (2x 37,5h) 75*50€=3750€

Yhteensä ensimmäisen vuoden aikana säästöjä siis kertyi noin. 37.000€

Säästöt on laskettu hinta-arvioilla, eikä niissä ole mukana opinnäytetyön toteuttamiskustannuksia.

Työ ylitti odotukset ja työssä oli nähtävillä insinöörimäistä tutkimus- ja kehitystyötä.